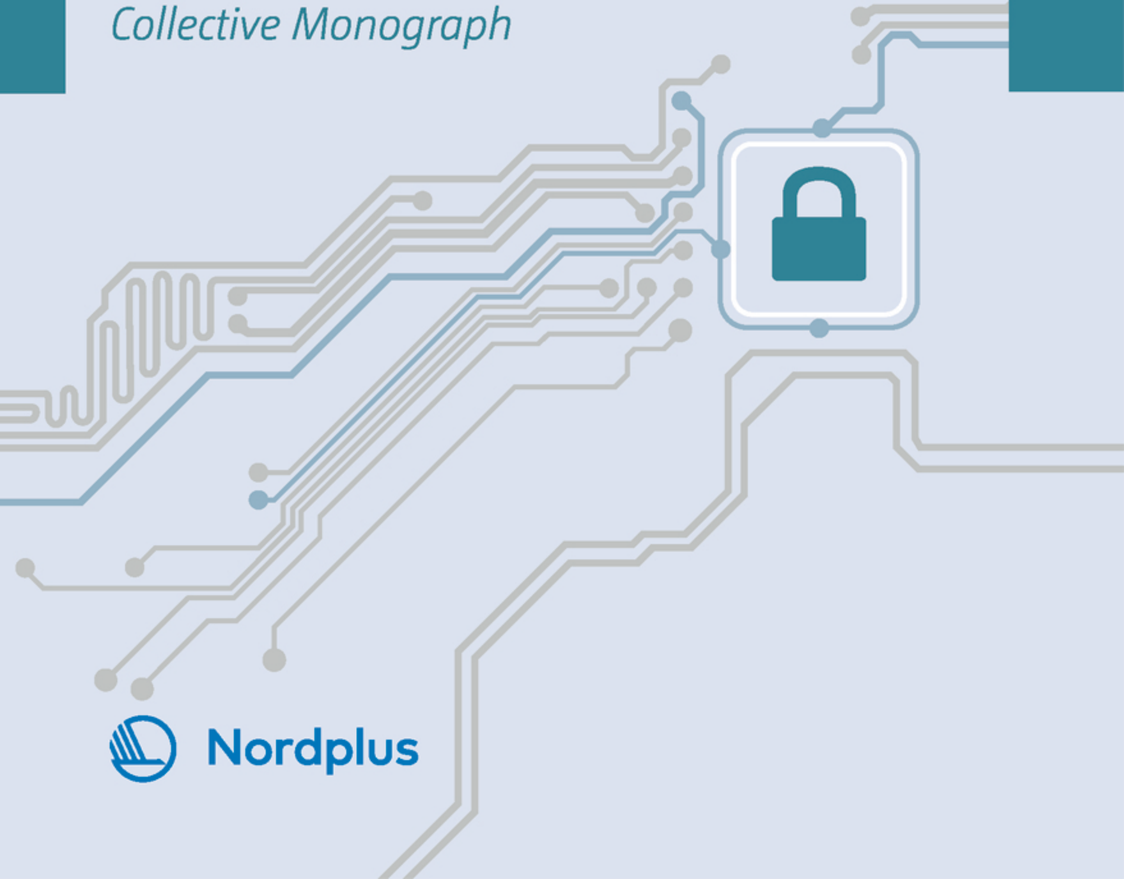
ORGANIZATION AND INDIVIDUAL SECURITY

Collective Monograph



Nordplus

ORGANIZATION AND INDIVIDUAL SECURITY

Collective Monograph

Edited by *Ivita Kīsnica*

This book is created with financial support of NORDPLSU higher education development program in frame of project "Development of Society and Organisation Security Programmes 2017", project number: NPHE-2017/10115

Project is implemented by following academic partners:

Riga 2018

Organization and individual security

Collective Monograph

Edited by ***Ivita Kīsnica,*** Vice Dean of Law Faculty, Turība University, *Latvia*

Contributors

Kaci Bourdache, Senior Lecturer, Laurea University of Applied Sciences, *Finland*
Raimundas Kalesnykas, *PhD,* Professor, Kazimieras Simonavičius University, *Lithuania*
Vilnis Veinbergs, Lecturer, Head of Internal Security Department, Turība University, *Latvia*

Scientific editor

Ingrīda Veikša, *Dr.iur.,* Professor, Head of Law Department, Turība University, *Latvia*

Reviewers

Anna Budnik, PhD, LL.M., Associate Professor, University of Białystok, *Poland*
Jarmo Heinonen, PhD, LicSc, Principal Lecturer, Laurea University of Applied Sciences, *Finland*
Dainis Mežulis, *Dr.iur.*, Associate Professor, Baltic International Academy, *Latvia*
Giedrius Nemeikšis, *Dr.iur.*, Lecturer, Panevėžys University of Applied Sciences, *Lithuania*
Dalia Prakapienė, *PhD*, Associate Professor, General Jonas Žemaitis Military Academy, *Lithuania*
Sigita Šimbelyte, *Dr.iur.*, Lecturer, Panevėžys University of Applied Sciences, *Lithuania*
Jānis Teivāns-Treinovskis, *Dr.iur.*, Professor, Daugavpils University, *Latvia*
Vladas Tumalavicius, *Dr.iur.*, Lecturer, General Jonas Žemaitis Military Academy, *Lithuania*

ISBN 978-9934-543-18-0
© Turiba University, 2018, 568 p.
E-mail: jf@turiba.lv
Printed by Ltd “Drukātava”

Contents

Introduction

Nowadays the rapidly advancing technologies and the ongoing changes in the socioeconomic and political processes in societies have stipulated an increased attention to security issues. In its broadest sense, the notion of security affects each and every member of society. At the age when the majority of borders are open in the direct and indirect sense of the word, the possibilities of humans and technologies become increasingly limitless. However, these opportunities are often not directed positively, but are rather targeted at causing harm to others. In this case, we can talk about both: sensitive migration issues and acts of terror, as well as about human interrelationships in general. It is no secret that we feel at our best in an environment, which is comfortable to us. Thus, any larger or smaller disturbance creates a sense of alarm due to the feeling of threat to one's own security as well as the desire to protect oneself. Security (being secure, protected against failures, fears, aggression) occupies a prominent second place in Abraham Maslow's pyramid of the basic human needs, closely following such physiological needs as food, sleep, rest and others. Therefore, paying attention to even the tiniest potential threats is a priority for everyone and generating response taken at an individual level and organisational level.

By starting already with the historical development of security throughout centuries and ending with cybersecurity, the book addresses issues related to individual security and the security of organisations. The articles provide an insight into the notion of security, its concepts in the global world, ethical issues of security, risk and quality management and leadership. They also address issues of physical guarding services, Schengen Area, fire safety, video surveillance and others. A separate chapter is devoted to security training as well as crime prevention, whistleblowers and cybersecurity.

The book has been developed as part of the "Development of Society and Organisation Security Programmes 2017" project (Project No. NPHE-2017/10115) and has brought together authors from three institutions of higher learning - Turiba University (Latvia), Kazimieras Simonavičius University (Lithuania) and Laurea University of Applied Sciences (Finland). It aims to clarify various issues related to the security of individuals and organisations and targets everyone interested in gaining insight into various security-related issues from the perspective of scientists and practitioners of Latvia, Lithuania and Finland. However, it should be noted that those interested in in-depth studies of security would require further reading, since the book does not aim at becoming a comprehensive source of information on all subjects, but rather provides an insight, raises general awareness and understanding of the issues and hopes to generate interest for further studies. Each article can be read as a separate issue.

Ivita Kīsnica

ASPECTS OF SECURITY IN THE HISTORY OF LATVIA

Guntis Zemītis

This article describes the historical experience of Latvia in ensuring safety and security. The article starts with an examination of the prehistory period up to the late 12th century, during which time the territory of Latvia was inhabited by ethnic groups that later formed modern Latvians. The history of Latvia is part of the history of Europe and has been touched by the same processes as the rest of the Europe, but on the other hand the experience of Latvia is unique. Here the political power has changed many times and these changes have occurred not only in the result of military confrontation, but have been also influenced by the ideological and social-political tendencies and by overdue or untimely political and economic reforms. The historical experience of Latvia shows the complex character of the provision of security which is the responsibility of both the security providers and each individual. The course of history demonstrates the ever increasing role of an individual in ensuring security.

Keywords: the history of Latvia, safety, security, security circles, security providers

THE BASICS OF SECURITY THEORY

Leonīds Makans

The development of society occurs when individuals who form it can choose the way they live and to do it in full.

One of the preconditions for a successful development of society is human freedom from fear and from want, which is generally understood as forming the notions of human security and human securitability as one of its forms of manifestation: a capacity to adapt to a rapidly changing environment.

The consequences of the sense of threat can manifest itself as a high degree of anxiety, depression and other diseases, including addiction to alcohol and drugs, criminal behaviour and in the extreme case: suicide. It can affect each member of society regardless of his/her social status. The ongoing processes in the world – technological progress, globalisation, expansion of extremism and terrorism bring about increasingly new conditions that need to be addressed.

Therefore, in order to improve the sense of security in the contemporary society and in each individual, it is important to understand the notion of security and the factors affecting it. It is particularly necessary for those representatives of state and non-governmental organizations that deal with one or another set of security issues.

The "Security Theory" study course, which has been designed for employees engaged in these issues, addresses and clarifies the main security related notions: threats, their subjects and their classification. The course also addresses the key types of security: security of power, social security, societal security and criminogenic security as well as separately: ecological, informational, cultural and moral threats and their characteristics.

Keywords: human securitability, security, threat, damage

SECURITY CONCEPT IN A GLOBAL WORLD

Raimundas Kalesnykas

In various resources, we can meet a number of academic studies that have defined the concept of security. Security by itself is multi-dimensional in theory and diverse in practice. Multi-dimensional approach of the security role in society and industry shows that a diverse understanding of a definition of security prevails. Current concept of security is so broad as to be very hard to find a reference point. Particularly, when we try to associate the security concept with individual security, organization security, public security, national security or international (global) security.

Nowadays, security has become a key factor in ensuring a high quality of life in society, guaranteeing respect for human rights, the rule of law and solidarity in protecting our critical infrastructures through prevention and tackling of common threats. The author takes an approach that the context and function of security is uninterrupted, but its scope, content and implementation forms can and must be vary taking into account the extent of society's development.

Academic studies on security development have undergone a fundamental shift over the past decade. States and organizations highlighting the common security threats, i.e. terrorism, manifestation of extremism and radicalism, cyber-crime, illegal migration, business spyware, money laundering, violation of data protection, corruption, etc. Accordingly, organizations must be ready for searching the new ways to manage their security threats and admit all challenges in the process of maintaining security. Many security risks and threats are continuous in nature and it is very difficult to eliminate them, which is why the security issues remain problematic. Only permanent and integrated efforts can ensure their minimal likelihood of becoming *threats and prevent adverse effects in the economic, social, ecological or other fields.*

The question for the EU countries and organizations today is what kind of security concept to use in promotion of common standards of ensuring their protection from security threats. Consequently, in 2016 EU changed approach to security, which led the transition from the regional perspective to global vision for ensuring security of its citizens and territory. Member States and organizations should clearly reflect the search for a better institutional framework on which to build a public–private security partnership.

Keywords: security definition, security globalisation, security threats, risks and challenges, security strategy

GUARDING SERVICES

Kaci Bourdache
Uģis Začs
Stanislav Dadelo

In addition to structural security and technical surveillance systems, people are needed to use, monitor and complement them. Only that way an organization can truly trust that their physical security is up to the challenge. Guarding services, which in most countries are regulated by law, are an effective option for this. In addition to outsourcing being a financial decision, guarding services provide specially trained and equipped security personnel with special rights. If security services answer the needs of their client base, they provide a multitude of options to manage various security and safety risks, not only in the domain of physical security but in e.g. emergency preparedness, information security and occupational safety as well. These services vary greatly and have options from a variety of around-the-clock static guarding to more affordable periodic rounds, where guards verify the status of the premises and perform individual, time-bound tasks. Via security technology, remote viewing and control services offer another affordable option. Lastly, specialized services such as close protection, cash and valuables transport and private detective services offer specific services for specific, security-intensive needs. The other side of the coin – being in the business of providing security services – requires high levels of integrity, professionalism and compliance of laws.

Keywords: physical security, security services, guarding services, security guard

RELATIONSHIP OF RISK AND QUALITY MANAGEMENT

Tuomas Wuorikoski

Risk and quality management are crucial factors in organisations' success regardless of the field of industry or sector. This article presents relationship of fundamental concepts, requirements for risk and quality management and best practices. The article is based on International Organization for Standardization's standards and author's experience of risk and quality management.

It is fair to define that managing risks and quality is the paradox of success, there will not be one without other. Risk and quality management must be an integrated element of operations, which can be done only if the organisation is able to define objectives (understanding the organisation), how to reach those (quality management), and phenomena to avoid and opportunities to seek (risk management).

One of the most powerful methods in risk and quality management is to use scenario-based methods due to understanding and creating an organisation's future being more and more crucial in a rapidly developing business environment. Megatrends are shaping the future more than ever and that increases the significance of risk and quality management.

Keywords: risk, quality, risk management, quality management

PUBLIC-PRIVATE SECURITY PARTNERSHIP

Raimundas Kalesnykas

The philosophy of public-private security partnership has been changed by substantial challenges for each society, political and economic instability in the "exposed to risk countries", a wide range players in security market and a rapid development of private business. Reasons of widening public-private partnership model are linked to globalisation and marketisation of security industry. The author's analytical research focuses on an analysis of outcomes highlighting challenges of governance security industry faced by Member States.

Each year private security industry across in EU represents 1.9 million jobs (or 325 private security officers per 100 000 inhabitants, 45,000 companies and annual revenue of € 40 billion). Private security companies are providing more and more various range of security services, which are traditionally been considered as a competence and responsibility of police and other public security agencies. Today we are faced with a situation that clearly shows the lack and/or differences of legal regulation of private security, common requirements for security business development, and risks of development of the public-private security partnership. On the other way, global challenges for security require to re-think an approach for the public-private partnership as integral and complex security mechanism. Many EU states present the public-private partnership model as a security guarantor that brings harmonization of law, code of ethics and standardization of security services.

Accordingly, the main task for the research is to identify the most significant problems arising in the implementation of public–private security partnership model across Member States with different security traditions. Provision of public-private partnership in security industry *may also be a business, the distinguishable feature of which is that the efficiency of the security services depends on competition between public and private security agencies. The establishment of universal regulatory mechanism for security business and public–private partnership would allow to prevent such type of business mode from negative trends. Public-private security partnerships are becoming more and more diverse and complex. In fact, public–private security partnership would allow creating a unique theory and practice of its own implementation and would be a basis of governing the security services providers. In order to achieve this vision it is necessary to determine the strategy of development of the security industry and to forecast conceivable dangers and risk in Member States.*

Keywords: security styles, security market, public security, private security, security partnership

THE BASIC CONCEPTS AND STYLES OF LEADERSHIP FOR SECURITY SPECIALISTS

Olena de Andres Gonzalez

Leadership plays an important role in the work of a security specialist. This article deals with defining the notions of a leader, leadership and explaining the difference between a leader and a manager. The description of power, its types and the basic concepts of leadership are provided. Leadership based on emotional intelligence and transformational leadership, the peculiarities of applying those styles of leadership and the recommended principles of leadership in the context of providing security have been addressed in detail. An integrated approach towards studying of leadership will equip security experts with tools for a more efficient interaction with their associates as well as for planning and for organizing security measures at a company level. The purpose of this article was to review and to generalize the basic definitions, concepts, theories and styles of leadership on the basis of existing research and to use the obtained results in the practical work of security specialists.

Keywords: leadership in security, leadership concepts, power, emotional intelligence, transformational leadership

PROFESSIONAL ETHICS

Ivita Kīsnica

The public has the right to demand that everyone, including state officials, legal professionals and regular employees of security services act in an ethical manner and that the privileges related to a formal official position are not used for personal gain.

Representatives of various professions face increasingly high demands in terms of ethics, which are based on such principles as openness, accountability, transparency, and objectivity. Public expects that state officials, legal professionals, representatives of security services and professionals of other areas while performing their duties, will consider public interests as a priority.

In practice, we often have to face many different situations, when in daily activities ethics is forgotten, including by security service personnel and these days such cases have also been made public by the media.

Ethical conduct is one of the key preconditions for the prestige of companies/institutions.

Keywords: ethics, security, corruption, security personnel

VIOLENT EXTREMISM AND RADICALISATION

Tuomas Tammilehto

Radicalisation, violent extremism and terrorism are much researched, but often poorly understood intertwined phenomena. Albeit, the risk of becoming a direct victim of them is very low, they are omnipresent in the contemporary world, including working life. Thus, they need to be taken into account in safety, security and risk management.

This article will present the three phenomena, discuss the differences between them as well as the commonalities, and present possible arenas for counter-measures in today's working life. Specific emphasis is put into the radicalisation process, and into two theoretical point-of-views: Routine Activity Theory and Situational Crime Prevention. The first stresses the importance of daily routines and encounters of human beings in all action, including maleficent. The latter serves as the fundamentals when thinking counter-measures. Furthermore, above theories suits well into working life, since many workplaces are, besides being places for business, quotidian meeting places that offer and enable e.g. socialisation, grouping and communication. Also, the core principles of the theories can be applied in working life.

Ultimately, this article brings understanding of human wrongs that are affecting us all.

Keywords: radicalisation, violent extremism, terrorism, working life, routine activity theory, situational crime prevention

EU INTEGRATED APPROACH TO RESPOND CONFLICTS AND CRISIS

Petteri Taitto
Kirsi Hyttinen

European Union is a regional security actor, as it has been founded to safeguard the security and prevent war in Europe after the Second World War. EU has evolved to security union and one of the founding documents along the Treaty of the Union is the EU Global Strategy, which sets the goals, priorities and ambitions when placing EU to the global scene and world order. One of the Global Strategy priorities is EU Integrated Approach to respond conflicts and crisis, which addresses all dimensions and stages of a conflict. Integrated Approach sets a particular emphasis on early warning and early action before a crisis erupts.[1]

The Integrated Approach outlines how to ensure rapid and effective crisis response, from building greater synergies between the different EU institutions, how to conduct Common Security and Defence Policy (CSDP) crisis management in line with other EU capacity-building missions and operations. At the same time, a greater emphasis will be paid on civil protection and humanitarian issues, and ensuring their link to development policies. In addition all mechanisms are subsequent to the political processes, including trade and even sanctions policies of the EU.[2]

This article gives an overview on how EU manages crisis globally and in particular in its neighbourhoods. The article presents EU crisis

[1] A Global Strategy for the European Union. (2016). Retvieved from https://europa.eu/globalstrategy/en

[2] An Integrated Approach to external conflicts and crisis. 7 June 2017. European External Action Service 10054/2017

response mechanism and its future prospects, and gives examples of the successes of Integrated Approach. The methodology is based on the literature review and interviews in the project “Improving Effectiveness of EU Conflict Prevention, IECEU”.

Keywords: European Union, integrated approach, EU external security, common security and defence policy

WHISTLEBLOWING – GROWTH OF SOCIETY

Jānis Veinbergs
Vilnis Veinbergs

This article is devoted to the issue of public engagement in promoting openness by forming the whistleblower institution. By raising the issue of those persons engaged in whistleblowing the article, therefore, promotes the opportunity of informing in good faith about possible violations, which according to whistleblowers can harm public interests. The objective of the article is to review the required public reaction given there is a chance to report about violations and to consider the means of forming a clear understanding in the society on the consequences of illegal actions, as well as to learn about the goals and conditions in terms of the respective draft law prepared by Latvian officials and experts. The article introduces readers to a study conducted by "Transparency International" on the development of the whistleblower movement in Europe and provides an insight in securing anonymity of whistleblowers.

By studying the causes of corruption, its manifestations and by making use of cultural and historical materials, the article presents corruption as an evil which requires the establishment of legal responsibility.

Public engagement in the fight against corruptive activities or against inaction towards it should be developed by means of various tools at public disposal. Based on the experience of the authors, the article pays particular attention to those personal motives, which preclude or vice-versa – promote whistleblowing.

Keywords: corruption, public threat, whistleblower, information

CRIME PREVENTION AND INVESTIGATION

Ryšardas Burda

Crime constantly accompanies any society. There is no doubt that the security of entrepreneurship and the safety of the enterprise are linked to social processes in society. Therefore, the security of the organization and the individual is linked to public safety and the state's ability to control crime.

In this section we will review the aspects of crime prevention and crime investigation. These aspects will be addressed in the context of organization and individual protection.

Preventing (preventing) crime plays an important role in the implementation of crime control.

Prevention means preventing, avoiding certain undesirable phenomena, processes, actions. Prevention is often accompanied by activities aimed at reducing the damage caused by criminal acts.

Prevention of violations of law is understood to have an effect not only on criminal offenses, but also on other types of legal proceeds of crime, illegal species and their determinants. These may include administrative violations, disciplinary offenses, civil legal violations, violations of procedural law.

Prevention is always against the commission of a crime. Prevention also minimizes crime damage. The legislator is criminalizing more and more acts. The level of crime with temporary fluctuations is increasing. The main objective of crime prevention is to protect the rights of citizens, society and the state.

Crime prevention will be addressed in the context of the organization's safety workforce. The proper communication of the organization's security staff with the police and other legal entities is very important.

It is understood that each state has its own criminal code or its own individual criminal investigation process. However, there are common police and security staff communication skills. Logic of action: from detention of an infringer to police call and participation in criminal proceedings at the prosecutor's office and in court.

Keywords: crime prevention, criminal code, criminal investigation, organization security, investigation

METHODS OF STUDYING SECURITY

Harri Ruoslahti

Security management is a broad field. One trend is that modern security solutions are increasingly technical, and can be considered cyber-physical systems. Studies in security management draw methodology from various fields of science, quantitative and qualitative, and applied approaches like engineering and service design. Co-creative methods help include views from industry, academia, and especially end-users.

The method of this paper is based on colleagues and students are included in co-creation of exploring available research methods. The innovative use of methods and elements from a wide range of disciplines are available for the research design. Co-creative methods include the views of multiple actors to create new knowledge and innovation, as end-user organizations have different interest groups, who should be included.

Security management supports society, its functions and businesses. Aims for security research, thus draw from the strategy of whom it supports, the company strategy, programs for national security, and on an EU-level programs such as the Horizon 2020.

Keywords: security, research, development, methods

SECURITY TRAINING STANDARD AS A TOOL FOR UNIFICATION OF PROFESSIONAL COMPETENCES AND REQUIREMENTS FOR PRIVATE SECURITY EMPLOYEES

Raimundas Kalesnykas

The quality of services provided by private security employees are determined by acquired knowledge, developed skills, gained abilities and provision of values. Academic studies examines the scope and content of employee's professional competence in security field, impact of professional training to the quality of security services, raises problems of searching common regulatory requirements for security services providers in Member States and discuss a need to have the necessary (specialized) education for working in the security area.

At first glance, it seems that in the EU exists a single understanding about the legal status of private security employees, but the research studies reveals the domination of various professional requirements for security personnel and different regulatory standards as well as a diversity of security personnel training and education. Legal status of private security employees is influenced by a constantly changing social, economic, technological or risk-based community environment, which raises new objectives for security employee's profession and defines the professional criteria according to the customers' needs of such services.

Member States still has no general security training standard, which would legitimize and unify security employee's areas of activities, professional competences, learning objectives and assessment methods of professional competences. Variety and loopholes in normative regulation causes practical problems of private security employees training, when trying to speculate what professional knowledge and competences they need, what evaluation criteria is necessary to *determine and how to assess their competence. Society is increasing the requirements for private security employees such as professionalism, competence, integrity, accountability and responsibility, publicity of activities, etc.*

The author adheres the provision that the absence of a clear methodology of defining the professional competences and setting common requirements for private security employees causes the mistakes of performing functions and providing security services to various clients. These issues are based on the evidence provided through research methods such as document analysis, comparative analysis, problem analysis and determinant analysis, which clearly shows that the security employees' education and training problems are indeed relevant. Member States could start discussions about the development of security training standard for all employees involved in the private security market, as well as the harmonization of common requirements and legal status for all security employees.

Keywords: security employee, professional training standard, competence, qualification

GUIDELINES FOR SECURITY STAFF TRAINING AND EVALUATION COMMUNICATION

Stanislav Dadelo

Private security is one of the key public safety factors in the modern world. Business community recognizes that their business success often depends on the professionalism of security officers. Private security staff assumes responsibility for human life and private property. Security officers professionalism covers general knowledge, and skills, and abilities that are essential for doing your job and work experience in the area of protection. It is important to set guidelines for evaluation and training security staff. This will require an attempt to define standards and goals of the private security industry. Necessary to define as an indicative instrument like a key document used by justice officials, members of the private security community, private security services and citizens. To achieve this aim it is important to set universal standards criteria and objectives for the private security sector. Training should be mandatory in all security activities areas and levels. Necessary to identify of governance professional certification programs in the public and private levels. Private security employers must develop job descriptions and instructions for each private security position. Learning programs should be designed in relation to the security staff job functions to be performed. Security staff employed as a guard or watchman, armed courier, alarm system installer or servicer, or alarm respondent, should successfully of formal training programs. Private security employers should ensure that private security personnel have ongoing training and are evaluated. A government agency should have the responsibility to accredit training private security schools, approve training syllabus, and certify instructors.

Keywords: staff, training design, evaluation criteria

STRUCTURAL SECURITY

Ryšardas Burda

For each state, the company or public safety has not only technical aspect of safety, but also social and legal aspects.

The social state aspect of safety of public use with conditioning of community (whether it be the village, the city or the whole state), the companies (in this case can be state or the municipal enterprise, private business (small, average or big and international)) or the person, with their individual (apartments the house, a private zone of expectation) requirements and interests. It can be economic and social aspects of development. In the social sphere with the development of the process a considerable community is necessary for the safe and viable environment. The economic space of activity of the company is more successful, more and more attention is paid in many various methods of management of risks. These risks can be internal or external. External risks are connected with the company environment where the company is also trust. Internal risks are connected with reliability of employees and internal space of the company on a number of safety issues. These and other aspects of the management and the technical equipment necessary are represented for consideration in this section.

Keywords: company risk, security principles, economic security, security structure, personal and property security, detective activity

SECURITY OF SCHENGEN BORDERS

Laura Tarkkanen

Schengen was established by signing of the Schengen Agreement in 1985. The Schengen Area is a territory where the free movement of persons is guaranteed. Schengen Borders Code defines that common measures on the crossing of internal borders by persons and border control at external borders should reflect the Schengen acquis, body of law, which serves as a basis for cooperation. The main measures under the Schengen cooperation cover matters such as asylum, visa and immigration policy and police co-operation. Border control in Schengen Area comprises not only border checks, but also an analysis of the risks for internal security and of the threats that may affect the security of external borders. To enhance the security of the Schengen Area, there are large-scale IT systems such as Schengen Information System (SIS) and Visa Information System (VIS) as tools for collecting, processing and sharing information in order to reinforce the external borders of the Schengen area.

Keywords: Schengen, Schengen borders code, Schengen member states, smart borders

VIDEO SURVEILLANCE SYSTEMS

Vilnis Veinbergs
Dainis Siliņš

The article contains a collection of information on various types of video surveillance cameras and equipment, the conditions for their use and provides recommendations on choosing and usage of a video system. Video surveillance should be considered as one of the main elements of guarding and security support, which is used in both – public and private sectors. In older times, when such systems did not exist, the defences utilised outpost guards and observers who, in case of danger, lit fires or found other means of informing the chief guard. Today it would be difficult to find a person in a civilised world, who would have never got in touch with the "glass eye" of a camera lens. The main advantages of video systems lie in their remote surveillance and data recording capability. With technologies developing, video cameras are available in various shapes and sizes, while data obtained by video recording systems are of a very high resolution and in excellent quality, allowing to differentiate a surveillance object, for instance, a person by using specialised data processing software, recognising a person by the typical facial features and thus substantially increasing a possibility for disclosing various illegal activities. In the course of the past twenty years, the rapid development of video surveillance equipment has been perfected and equipping a protected object with video cameras no longer posing any difficulties. However, taking into account the values of a democratic society, which is based on law, one should respect the basic rights of physical persons, particularly the inviolability of their private lives, regulated by the normative acts of the EU and its member states.

Keywords: security, video surveillance cameras, video surveillance systems

FIRE SAFETY SYSTEMS

Uģis Začs
Viktorija Ratačova

Fire safety is one of the key security risks, which should be paid close attention already during the design phase of a facility. The main fire safety feature deserving careful attention is a timely detection of fire or fire threats and notification of people on the beginning of an emergency situation, in this case – fire. Automatic fire detection and alarm system is particularly important in the cases when a dangerous situation is formed in a building visited by a large number of people, and the visitors need to be notified of the threat. Malfunction of the system or its improper installation and service can lead to a grave tragedy, experienced by the Russian city of Kemerovo on 25.03.2018.
In this chapter, the authors review and describe the following fire safety systems:

1) automatic fire detection systems;
2) automatic fire extinguishing systems;
3) voice notification systems.

Keywords: fire, fire hazard, fire safety systems, alarm, emergency, staff on duty, automatic systems

ACCESS CONTROL SYSTEM

Uģis Začs

A correct and thought-out procedure of access to a facility and movement inside of it is one of the integral parts of the development of a security concept for a facility. Nowadays, there are various technical solutions and systems available, which are targeted at decreasing an opportunity for human error and the engagement of people in controlling this procedure. In this chapter the author reviews and describes several technical solutions, which help and ensure a controlled access to a facility. The author provides an overview of both – simple solutions and more complex multifunctional systems. This chapter deals with issues of how to approach access control systems, how to choose the most economically viable solution for gaining maximum effectiveness from the system selected. In addition, the functions and gains from the contemporary access control system are also provided.

Keywords: access, control, registration, access control, access control system, restriction

SECURITY GUARD MANAGEMENT CENTRE

Uģis Začs
Dzintars Rendenieks

Fast and operationally effective exchange of information and coordination is important to an organised guard group or a company. In order to provide effective exchange of information and coordination of security measures, there is a need for a specific place, which provides complete access to information, as well as facilities for conducting daily operations. A security guard management centre, which at stationary facilities is also referred to as a security control room or a security switchboard, is a place where all information on a facility and a group of facilities is being collected. While constructing such a place, it is important to be aware that a management centre must enjoy maximum security against potential access by outsiders. One must also make sure that the centre operates on a 24/7 basis.

In this chapter, the author reviews the establishment of a management centre, the legal framework of its functioning and maintenance, as well as the requirements of the Latvian and EU legal standards. In addition, the author provides an overview of the greatest risks and problematic issues, which can be faced in the course of operation of a management centre. This should assist the employees of the security industry in raising their awareness of the issues and should provide information on how to approach individual situations.

Keywords: MSS, main security switchboard, security guard management centre, security, exchange of information, operational effectiveness

CYBERSECURITY AND RESILIENCE IN A SOCIETY

Julia Nevmerzhitskaya
Jyri Rajamäki

Digitalization has changed our society in the last decades. Today both public and private sector, critical infrastructure services, companies and citizens increasingly depend on IT networks and data processing infrastructure in their everyday activities. At the same time the digital age has also increased the threats related to cybersecurity issues and privacy breaches, and increased the probability of cyber-attacks to critical assets, networks and systems that sustain a nation's safety and prosperity. Understanding the consequences of cyber-attacks to a critical infrastructure requires a shared responsibility among national and local entities, public and private owners and operators, and the IT hardware and service providers in their value chains. This shared responsibility is a key to achieving cyber resiliency in a society, in order to prepare for, adapt to changing conditions, and recover from cyber-attacks. This article focuses on understanding cyber resiliency in a society. It describes how societies can develop cyber resiliency capabilities by mitigating threats, increasing awareness, and balancing between privacy and security.

Keywords: cybersecurity, societal challenge, cyber threats, resilience

CYBERSECURITY IN AN ORGANIZATION

Jyri Rajamäki
Julia Nevmerzhitskaya

As the scale and complexity of the cyber threat landscape is rapidly evolving, with increasing number of cyber-attacks on all types of organisations, the pressure on the cybersecurity resilience of organizations is also gaining importance. Organizations face a number of ICT security risks on a daily basis. To defend themselves against cyber threats, they need to leverage its people, information and systems to protect organizational assets against threats via ICT. By investing in the people and their education, digitizing and encoding information and processes, and technology that is necessary to transmit data, organizations can become more resilient. This article describes the human-data-technology model of organizational cybersecurity, and argues that cybersecurity goes beyond the risk management process to be a shared responsibility of leadership, ICT staff, and other personnel. When properly taken care of, cybersecurity can be turned from risk to opportunity that improves business continuity, enables access to new markets that have requirements for cybersecurity and answers to the regulatory requirements affecting products and services.

Keywords: cybersecurity, organizational security, risk management, business continuity, organisational resilience, resilience management

CYBERSECURITY: HOW TO STAY SAFE IN THE CYBERSPACE

Elina Radionova-Girsa

While staying open to the new technologies people do not only receive different opportunities and bonuses from it but also get threats. Some of them from the first sight seem to be easily resolved but unfortunately, they can cause serious consequences. Talking about cyberspace one should understand that it is something more than a place to study, communicate, entertain yourself, do shopping, surf and find information. It is a place where we leave our tracks – personal data, bank account data, work related documents, etc. Cybersecurity can educate people and help them to go through mentioned treats.

On the one hand, cyberspace does not have any limitations and borders. Threats and attacks can come from every part of the world. But from the other hand, countries and unions are trying to provide a protection to their citizens in a different way. The main goal for the research is to find out the main cybersecurity approaches worldwide and compare it to the Baltic States regulations. Such methods as comparative analysis of regulations on cybersecurity, scientific literature analysis and doctrinal analysis were used during the research. Results can be used both in a theoretical way and in practise in order to understand cybersecurity problems and character of legal regulations among Baltic States Countries.

Keywords: cyberspace, cybersecurity, cyber-attacks

Part I

SECURITY THEORY

ASPECTS OF SECURITY IN THE HISTORY OF LATVIA

Guntis Zemītis

Introduction

The term “security” is a very wide one. The threat to the security can come from outside or from within. Danger and peril has accompanied a human being since the dawn of the mankind. Nature has threatened the human with unexpected climate changes, rainstorms, cold and heat, earthquakes and volcanoes. With time people have managed to substantially lessen threats imposed by nature, but nevertheless time after time the elements give a reminder that nature simply is superior to man. One such reminder is the loss of ferry “Estonia” and 852 lives on board on September 28 1994 in the waters of seemingly so small and safe for shipping Baltic see. People have won a supremacy over other species and have imposed restrictions on the misery caused by disease, but has not managed to escape the threat created by other people. The development of science has not only lessened, but also increased threats. Worry about safety will never cease. With the change of time threats change and so do the ways how to protect people. In our age changes happen so quickly that knowledge gained by young people at school are already outdated when they reach the employment stage. It is not possible to foresee what challenges people will face after ten or twenty years. In a very recent past, terms used today on an everyday basis like “cyberthreat”, “cyberwarfare”, “cybersecurity” did not mean anything. Should people in such conditions be interested in the methods their ancestor used to ensure safety centuries ago? It might seem unnecessary and odd. Nevertheless, looking back in the past is a direct means to avoid repeating the mistakes of the past, it gives a chance to notice regularities that have to be taken into account when caring for the safety of an individual or a country.

Methods used in this article are the historically genetic and problematic chronological approach. The aspect of security in the history of Latvia up until now has not been considered to any extent.

1. Security during Prehistoric period

At the dawn of the history *homo sapiens* united among themselves and formed small hunter-gatherer bands within which occurred not only spontaneous, but also regulated processes. Within a band a division of labour existed, according first of all to age and sex. In the regulation of conflicts, the third factor is important, which either prevents a conflict or forces to regulate it. It could be done either by a judge (a priest, a sorcerer or a shaman) or a representative of a public power. During times when public power was not yet formed or was still weak, the order was maintained by holding to a custom. Custom or common law is the upkeep of order without the intervention from state power. The guarantee for individual's safety was his kin. The kin demanded liability for the killing, mutilation, rape or injury done to their blood relative. Answer to a killing of one's kin was killing someone from the guilty party's family. Such rights are called vengeance rights. It is a blood feud following a principle "death for each one killed". German sources name this *Fehde* (older form – *faida*), the corresponding term in Latvian is *vaidi, vaidinieks, vaidu laiki*.

2. The end of Prehistoric period and the period of crusades (late 12th–13th century)

2.1. Individual safety during the end of Prehistoric period and during the Crusades period

The latest period of prehistory in Latvia lasts from the 9th to the 12th century and is called the Late Iron Age. Fragmented information about this period is available in Scandinavian and Ancient Russian written sources, but period from the middle of the 12th century is covered by the Livonian Chronicle of Henry[3]. This chronicle gives information about the beginnings of the crusade period as well, but events of the second half of 13th century are detailed in the Livonian Rhymed Chronicle[4]. Both chronicles give good notion about those dangers people encountered during late Iron Age and early Middle Ages. Without any doubt, one such danger was crime perpetrated by neighbours. Crime has existed in all times. In such cases it was still necessary to reckon with a reaction from the family and kin of the victim. The perpetrator had to reckon with blood feud if not in his generation, then in next ones.

During late Iron Age blood feud began to be substituted by a payment, the so called composition (Latin – compositio). Already

[3] Henricus Lettus (2000). *The chronicle of Henry of Livonia*. Translated with a new introduction and notes by James A. Brundage. New York: Columbia University Press. Edition 2003;

Indriķa hronika (1993). No latīņu val. tulk. Ā. Feldhūns; Ē. Mugurēviča priekšvārds un komentāri. Rīga: Zinātne, I; 10

[4] *Atskaņu hronika* (1998) = *Livländische Reimchronik* (1998). No vidusaugšvācu val. atdzejojis V. Bisinieks. Ē. Mugurēviča priekšvārds, Ē. Mugurēviča un K. Kļaviņa komentāri. Rīga: Zinātne

the German-composed Couronian peasants rights[5] which was the same as the peasant's rights of Riga archbishopric[6], rights of Livonians and Estonians[7], disclose the common law of peoples of Latvia, the Couronians, Semigallians, Lettgallians, Selonians, Estonians and Livs: the payment in case of crime is fixed in units called *ozeringe,* most likely meaning a small silver bar or stick. The rights mention notion "man money", namely, money to be paid in case of killing a free man.[8]

As far as it is possible to gather from the written sources, the role of judges was fulfilled by pagan priests or sorcerers (Latin – *oriolus*)[9].

If the danger constituted a hazard for the whole community, the justice was administered by the elders of the district. So Livs in Ikskile in their meeting (Latin – *placitum*) in 1206 sentenced two

[5] Stikāne, V. (2001). Kuršu tiesības jeb Kuršu un zemgaļu zemnieku tiesības. Retrieved from https://www.historia.lv/dokumenti/kursu-tiesibas-jeb-kursu-un-zemgalu-zemnieku-tiesibas-teksts-lejasvacu-valoda-un-tulkojums

[6] Latgaļu tiesības jeb Rīgas arhibīskapijas zemnieku tiesības. Retrieved from https://www.historia.lv/dokumenti/latgalu-tiesibas-jeb-rigas-arhibiskapijas-zemnieku-tiesibas-teksts-lejasvacu-valoda-un

[7] Lībiešu–igauņu tiesības jeb Livonijas zemnieku tiesības. Retrieved from https://www.historia.lv/dokumenti/libiesu-igaunu-tiesibas-jeb-livonijas-zemnieku-tiesibas-teksts-lejasvacu-valoda-un

[8] Stikāne, V. (2001). Kuršu tiesības jeb Kuršu un zemgaļu zemnieku tiesības. Retrieved from https://www.historia.lv/dokumenti/kursu-tiesibas-jeb-kursu-un-zemgalu-zemnieku-tiesibas-teksts-lejasvacu-valoda-un-tulkojum

[9] Henricus Lettus (2000). *The chronicle of Henry of Livonia*. Translated with a new introduction and notes by James A. Brundage. New York: Columbia University Press. Edition 2003;

Indriķa hronika (1993). No latīņu val. tulk. Ā. Feldhūns; Ē. Mugurēviča priekšvārds un komentāri. Rīga: Zinātne, I; 10

baptized Livs Kyrianu and Layanus to a deterrent death (to be torn to pieces).[10]

During the Iron Age the security of each group of peoples depended solely on the number of grown-up men. Each adult was a warrior. During late 13th century the main threat in Livonia were the Lithuanians, who were superior in numbers. According to the Chronicle of Henry, "…. The Lithuanians were then such lords over all the peoples, both Christian and pagan, dwelling in those lands that scarcely anyone, and the Letts especially, dared live in the small villages…".[11]

Main aim during a military expedition was to kill as many enemy men as possible; women and young girls "only one that the army is used to spare" on the other hand were driven into captivity to become either servants or mistresses. Possibly one of the main aims was to ensure that they do not give birth to sons – further enemies by staying in their home land.

2.2. Safety caretakers at the end of prehistoric period and during the Crusades period

The Chronicle of Henry describes ruthless campaigns in 1215 by Lettgallians (letts) under the leadership of *Tholowa* (also – Tolowa) and *Talibaldus* with their sons *Rameko* (also – Rameke) and *Drinivalde* to southern Estonia (*Ugaunia, Ungaunia, Ungania*): "They and their friends and relatives collected an army of Letts, and Brothers of the Militia from Wenden and other Germans went with

[10] Henricus Lettus (2000). *The chronicle of Henry of Livonia*. Translated with a new introduction and notes by James A. Brundage. New York: Columbia University Press. Edition 2003;

Indriķa hronika (1993). No latīņu val. tulk. Ā. Feldhūns; Ē. Mugurēviča priekšvārds un komentāri. Rīga: Zinātne, X; 5

[11] Ibid, XIII; 4

them. They entered Ungannia, despoiled all the villages, and delivered them to the flames… They sought out the Ungannians in the dark hiding places of the forests and the Ungannians could hide from them nowhere. They took them out of the forests and killed them and took the women and children away as captives".[12]

Similarly acted the elder of Stocele district Russinus in 1208, who "was the bravest of the Letts"[13], in the Estonian district Saccala (also – Sackala) and declared after a campaign: "The sons of my sons will tell their sons to the third and fourth generations how Russin wrought slaughter on the Saccalians".[14]

During the last part of the Iron Age certain changes in the status of the rulers occurred. For centuries the power of a ruler rested in his authority – a capability to convince and to lead. During the end of the period the power became hereditary. It is possible, that a dynasty of rulers existed in Semigallia. Nevertheless, for Baltic peoples the same as for Ancient Germans a ruler was first of all a military leader. The Livonian Rhymed Chronicle tells about a duel between the ruler of Semigallians Viestards and a knight named Markwart at a moment, when semigallians where surprised by the crusaders at a time of rest.[15] The fame of a successful military leader belongs to the ruler of Turaida Livs "as if king" (Latin: *quasi* rex)

[12] Henricus Lettus (2000). *The chronicle of Henry of Livonia*. Translated with a new introduction and notes by James A. Brundage. New York: Columbia University Press. Edition 2003;

Indriķa hronika. (1993). No latīņu val. tulk. Ā. Feldhūns; Ē. Mugurēviča priekšvārds un komentāri. Rīga: Zinātne, XIX; 3

[13] Ibid, XII; 6

[14] Ibid

[15] *Atskaņu hronika* (1998) = *Livländische Reimchronik*. (1998). No vidusaugšvācu val. atdzejojis V. Bisinieks. Ē. Mugurēviča priekšvārds, Ē. Mugurēviča un K. Kļaviņa komentāri. Rīga: Zinātne,1768–1785 Row

Caupo and to Semigallian rulers Viesthardus (also – Vesthardus, Vesthardus) and Nameyxe.

The support of any ruler was his military band (Latvian: *karadraudze*), named "relatives and friends" (Latin – *cognatis et amicis*) in the chronicle. They could as well be professional warriors.

During the campaigns warriors can be observed that stand out among others. Today we would call them elite troops or special forces units. The task of these was to inspire fear in the enemy before the fight. The Chronicle of Henry describes the siege of Vilande castle in 1210: "… they put on German armour, gotten during the first fight in castle gate, stood bragging at the very top of the castle, prepared for the fight and with their shouts bantered and mocked at the troops".[16]

An outstanding Lettgallian warrior was Roboam who during the siege of Beverin castle by Estonians in 1208 alone descended among the enemies, "killed two of them, and returned to his people safe and unharmed through an adjoining part of the fort…"[17]. Not less lucky was his brother Veko, who killed the leader of Saccala Estonians Lembitu, [18] but was killed himself the next year, albeit "… fought alone with nine Russian for a long time with his back to a tree. He was finally wounded from behind, fell, and died."[19]

Elite troops could also use unexpected methods and attack in small numbers in places, where the attack was least expected,

[16] Henricus Lettus (2000). *The chronicle of Henry of Livonia*. Translated with a new introduction and notes by James A. Brundage. New York: Columbia University Press. Edition 2003;

Indriķa hronika (1993). No latīņu val. tulk. Ā. Feldhūns; Ē. Mugurēviča priekšvārds un komentāri. Rīga: Zinātne, XIV; 11

[17] Ibid, XII; 6

[18] Ibid, XXI; 3

[19] Ibid, XXII; 3

similarly as it is today done by special operations forces. In 1206 when crusaders and Semigallians attacked the Satesele castle belonging to Livs, some of the crusaders and Semigallians tried to mount the castle from the other side, but were discovered and lost five of their number.[20]

The tactics of fighting generally was comparatively simple: during a fight the better prepared and more heavily armoured took the place in the centre, while others formed the flanks. But the security of people was not dependent only on the luck in the battlefield. It was also very important to receive timely knowledge about potential threats. News were delivered either through runners or envoys. As can be gathered from the Chronicle of Henry, local peoples received information about events in neighbouring lands quickly. The Chronicle mentions "skilful messengers" [21], meaning that such not only delivered a given message, but also gathered information to supplement it.[22]

[20] Henricus Lettus (2000). *The chronicle of Henry of Livonia*. Translated with a new introduction and notes by James A. Brundage. New York: Columbia University Press. Edition 2003;

Indriķa hronika (1993). No latīņu val. tulk. Ā. Feldhūns; Ē. Mugurēviča priekšvārds un komentāri. Rīga: Zin, X; 10

[21] Ibid, IX; 3

[22] Zemītis, G. (2010). Komunikācija Latvijā 12. gadsimta beigās un 13. gadsimta sākumā pēc Indriķa Livonijas hronikas ziņām. *Biznesa augstskolas Turība Zinātniskie raksti Acta Prosperitatis Nr. 1.* Komunikācija publiskajā telpā. Rīga: Biznesa augstskola Turība, p. 69

3. Middle Ages (13th–16th century)

The Crusade against the peoples of Eastern Baltic began in 1195/1196 with the bull of Pope Celestine III (*Caelestinus III*, around 1106–1198) and ended in 1290, when Semigallians burned their castles and moved to Lithuania in great numbers. Peoples living in nowadays Latvia and Estonia were baptized and feudal relations formed here quite like in the Western Europe. The name of Livonia itself is a latinised and germanised form of the Liv's land. Conquered lands were dedicated to the Holy Virgin Maria, who was considered the patron saint of Livonia. Crusades were common undertakings of the whole Christian world and as such were authorized by the head of the Roman Catholic Church. The leader of the Crusade to the Baltics was the representative of the Pope, the bishop of Riga (of Ikšķile at first).[23] The aim of the Bishop was to create in Livonia a state, where the bishop would be both spiritual and secular ruler. But as the Bishop was lacking in military power, the Livonian Brothers of the Sword military order was created to conquer the land. Giving in to the pressure of the Order, the Bishop of Riga allotted one third of already conquered lands to the order. The order demanded one third of the as yet un-conquered lands as well and as a result the Livonian Brothers of the Sword order became a ruler of the land side by side with the Bishop.[24] This gave the grounds for a conflict that lasted even beyond actual destruction of the Livonian Brothers of the Sword order in the battle near Saule in 1236. The remains of the order were incorporated in the Teutonic order (*Ordo fratrum domus Sanctae Mariae Theutonicorum*

[23] Eihmane, E. (2012). *Rīgas arhibīskapa un Vācu ordeņa cīņas par varu viduslaiku Livonijā*. Rīga: LU Akadēmiskais apgāds, p. 8

[24] Ibid, p. 10

Ierosolimitanorum, *Ordo Teutonicus*) which in its turn had received a papal privilege that gave it independence from all ecclesiastical or secular lords and subordinated it directly to the papal curia.[25] The Teutonic order accordingly did not acknowledge the Bishop to be the order's feudal lord and this caused political and military conflicts during the whole time Livonia existed. Capturing of enemy lands and castles was a commonly used method of fighting. Still the order used other methods as well, such as interception of envoys and letters which was carried out to minimize the Bishops chances of informing the Pope and the emperor about happenings in Livonia and asking for their help.[26]

The social structure of the local peoples did not change up to the late 13th century. During the 14th century a peasant class formed and consisted mainly of local inhabitants. A special peculiarity of Livonia was that each class lived according to their own rights and even used their own language: the official language of the clergy was Latin and ethnically the clergy consisted mainly of Germans, the language of knighthood was German, but peasants spoke local languages – Curonian, Semigallian, Latgallian, Liv and Estonian. In the later part of the Crusades and after a peasant class formed, peasants – meaning local people in general – were in most cases not involved in military campaigns anymore. The forces of the Teutonic order constituted main and the most stable military potential in Livonia and the only real force that could repulse larger attacks on the representatives of the Roman Catholic Church.[27]

[25] Eihmane, E. (2012). *Rīgas arhibīskapa un Vācu ordeņa cīņas par varu viduslaiku Livonijā*. Rīga: LU Akadēmiskais apgāds, p. 13

[26] Ibid, p. 27

[27] Ibid, p. 18

The importance of the Teutonic order was considerably lessened after the defeat at the Battle of Grunwald (also known as Battle of Tannenberg) in 1410, in which the Livonian branch did not participate.

Knighthoods role of a main military power and security guarantor started to diminish in the second half of the 15th century. A symbolic turning point was the defeat of Charles the Bold, Duke of Burgundy (*Charles le Téméraire*, 1433–1477) near Nancy on January 5, 1477 when lightly armoured Swiss–Lotharingian infantry units defeated the Dukes heavy armoured knights.

4. Modern period. Lesson taught from the dissolution of Livonia

4.1. Reformation

Changes in military were not the only ones that marked the transition to the Modern period. The Middle Age order was defined by the Roman Catholic Church. According to the theological doctrine about the order on earth imposed by one single divine will, the secular and spiritual realms of the world were separated. This separation was personified by the Pope and the Emperor; the power was dual in its nature, with Pope holding the spiritual instruments of power or *spiritualia* and the Emperor holding the secular instruments of power or *temporalia.* According to this view, harmony and justice could be ensured only by combining both instruments of power. [28]

[28] Levāns, A. (2013). Politiskās organizācijas modeļi viduslaiku Livonijā 13.– 16. gadsimtā: manifestācijas un leģitimācijas formas. *Latvieši un Latvija. II sējums.* Valstiskums Latvijā un Latvijas valsts – izcīnītā un zaudētā. Rīga: Latvijas Zinātņu akadēmija, p. 58

On October 31st 1517 a monk of the Order of Saint Augustine named *Martin Luther* (1483–1546) published his 95 theses in Wittenberg and the Reformation began. Regarding from the point of view of security – if the Catholic Church represented stability and order that had existed for hundreds of years, than Reformation was a threat to it. This threat was in fact created by the Catholic Church itself. The movement of the religious rebirth began at the time, when the reputation of Catholic Church was exceptionally low.[29] A reaction from the Catholic Church followed, which is traditionally called the Counter–Reformation. Today it is believed that "Catholic reformation" is a more appropriate term to describe those movements within the Catholic Church, that, although with delay, but still tried to solve the problems that had called forth the Reformation. [30]

The fight between the Roman Catholic church and Protestantism gave birth to new forces, which were even called "soldiers of Christ", although had in reality little relation to actual military warfare. A Spanish nobleman *Ignacio de Loyola* (*1491–1556) created The Society of Jesus, which was called "The Society of Jesus" or "The Company"* (compagnie de Jésus) but is more commonly known as the Order of the Jesuits. Demands one had to fulfill to be accepted in the Society were high. Loyola said that "we want to accept beautiful people with nice appearance, as it is determined by our own way of life and our relations with our akin". Jesuits could not have any side interests, their only goal and interest had to be the revival of Catholicism.

Jesuits had to be absolutely obedient to their chief: "Let everyone know, that those bound by the duty of obedience have to

[29] Deivis, N. (1996). *Europe a History*, 1996 = Deivis, N. (2009). *Eiropas vēsture*. Rīga: Jumava, p. 501

[30] Tēraudkalns, V. (2017). Reformācija starp mītiem un vēsturi. *Ceļš*. 2017, Nr. 68., p. 65

let their leaders treat them as if they were a corpse, which they can move around and do with it what they want".[31]

Protestants on their side mobilised for a fight with the "Catholic Reformation". It was especially noticeable in England during the reign of Queen Elisabeth I of England (1533–1603) from 1558 to 1603 with the strife between Protestant Elisabeth I and her rival to the throne, Catholic *Mary I of Scotland* (1542–1587). The principal secretary of Elisabeth I *Sir Francis Walsingham* (1532–1590) even created a secret service to oppose Catholics.

By translating the Scripture and by conducting religious services in the local languages, Protestants had gained immense advantage in the struggle over people's minds. Jesuits compensated that by advancing the progress of education and learning. An essential change had taken place – convictions of a man gained more and more importance in ensuring safety. The time, when only few could provide safety, was left in the past.

Transition from the Middle Ages to the Modern period in Livonia was marked by Reformation and the following Livonian War or the First Northern War and the collapse of Livonian Confederation. Livonia was one of the first lands where Reformation triumphed. In Riga Lutheranism had practically prevailed as soon as 1525. The victory of Lutheranism was one of, but not the only reason why Livonia collapsed. After the Reformation the structure of Livonia did not change and it remained a body of Catholic feudal dominions, although the subjects living there had already turned

[31] Vippers, R. (1930). *Jauno laiku vesture. 1. daļa. Atradumu reformācijas un reliģisko karu laikmets*: Latvijas Universitātē lasītais kurss. Tulk. I. Alksne un M. Rutmane, rediģējis M. Stepermanis. Rīga: Latvijas Universitāte, p. 207

to Lutheranism.[32] Feudal Livonia whose military security depended on only few hundred knights – the Order and its lieges, could not contest against Russian forces numbering several tens of thousands. After the end of the Crusades the social gap between clergy and knighthood from one side and peasantry from the other had increased. Largest part of the population, namely Latvian and Estonian peasants were rarely involved in fighting. When such involvement took place, the results were usually good. For example, *Ivo Schenkenberg* (around 1550–1579) successfully fought with Russians in Estonia and his military unit was composed of Estonian peasants. Similar were the proceedings of the administrator of Turaida Castle clerk Johann Büring, who captured Cēsis Castle in December 1577 with the help of 100 German and 80 Polish cavalry and 200 Latvian peasants. He later took the Castles of Burtnieki, Limbaži, Straupe and Nītaure as well. But obviously such cases were not given enough credit and the description of Johann Büring given by Balthasar Russow ends with such words: "He did much good for Livonia, but earned very little appreciation".[33]

4.2. The territory of Latvia at the possession of Poland and Sweden

During next centuries the territory of Latvia came under the rule of Poles and Swedes. The territories on the right bank – The Duchy of Livonia (*Ducatus Transdunensis*) was incorporated in Lithuania in 1566, but the Duchy of Courland and Semigallia (*Ducatus Curlandiae et Semigalliae*) (1561/1562–1795) formed on the left bank

[32] Ābers, B. (1940). *Latvijas tiesību vēsture.* Pēc doc. B. Ābers 1938./39. lekcijām. Rokraksta vietā, pp. 102, 103

[33] Rusovs, B. (1926). *Livonijas Kronika*. Ed. Veispala tulkojums. Rīga: Valters un Rapa. Retrieved from https://www.historia.lv/biblioteka/baltazara-rusova-livonijas-hronika, part, IV

of Daugava River were lieges of Poland. The security of the Duchy of Courland towards outside still continued to depend on the cavalry of former lieges – the country noblemen, including three cavalry companies enlisted by the Duke from his estates and 200 cavalrymen given by the noblemen. Even if this number was doubled in case of an emergency, the Duchy of Courland could not counter with the armies of neighbouring states, largely formed by hired mercenaries and much larger in numbers.[34] An attempt by Duke Jakob (1610–1682) to form an army of hired infantry did not succeed because of prejudices that peasants are not able to handle weapons, an army constituting of serfs can't be trusted etc.[35] Diplomacy performed by the Dukes remained the main guarantee to ensure the security of the Duchy. The existence of the Duchy was jeopardized by the lack of an heir to the Duke. For example, the childless Duke Fridrich (1569–1642) had to exert great effort to ensure that the throne goes to his nephew Jacob.[36] Change of dynasties could lead to dependence from more powerful neighbours – Russia, Sweden, Poland or Prussia or even full or partial loss of independence.

After the second division of Poland in 1793, Courland had lost its feudal suzerain and its days were numbered. On April 15 (26) the Empress Catherine II of Russia (*Екатерина II Великая;* 1729–1796) ended the existence of the Duchy of Courland and Semigallia and added former territories of the Duchy to the Empire of Russia.

[34] Jakovļeva, M. (2004). Kurzemes hercogistes militārā reforma un hercoga Jēkaba mēģinājumi to reformēt XVII gadsimta vidū. *Latvijas Kara muzeja gadagrāmata V*. Rīga: Latvijas Kara muzejs, p. 13

[35] Ibid, pp. 7–19

[36] Jakovļeva, M. (2013). Valstiskums Latvijas teritorijā agrajos jaunajos laikos: Kurzemes un Zemgales hercogistē. *Latvieši un Latvija. II sējums. Valstiskums Latvijā un Latvijas valsts – izcīnītā un zaudētā.* Rīga: Latvijas Zinātņu akadēmija, pp. 133–136

4.3. Changes in the provision of the security after the French Revolution

Next turning point in history that completely changed the concept of security in Europe was the French Revolution in 1789. Members of society became citizens that could participate in the settling of the destiny of a nation. The defence of their fatherland became a duty of citizens.

The territory of Latvia since 18th century gradually had come to be part of the Empire of Russia, which was not touched by democratic changes. The power of a monarch was absolute and by far the largest part of the inhabitants – the peasants were absolutely without any rights and in the full power of country nobility.

At first the three Baltic Governorates – Estonia, Livonia and Courland possessed certain autonomy. They were reached by ideological movements of the Western Europe, Enlightenment among others. The most visible result of the Enlightenment was the abolition of serfdom in Estonian Governorate in 1816, the Governorate of Courland in 1817 and in the Governorate of Livonia in 1819. Peasants in other territories of Russian Empire had to wait for the liberation until 1861. Starting with the agrarian reform in the year 1849 it became possible to buy land as private property. Still about half of the land remained in the hands of German nobility and correspondingly a social and national tension continued to last. Only small part of the peasantry could buy out their land and homes. The Soviet historiography evaluated the coming of Baltic lands under the rule of Russian Empire as a positive occurrence, remarking that it led to a long period of peace. This is only partially so. Latvian peasants had to provide recruits that had to fight in the wars of the Empire, while in 1812 Courland was touched by the campaign of Napoleon. Latgale (Inflanty) was added to the Russian Empire as part of Poland and so it remained closely bound with events in Poland. Part of the land nobility supported the Polish national liberation movement. Legendary fame was gained by Countess Emilia Plater (1806–1831), who during the Polish uprising of 1830 was in charge of a polish military unit in Latvia and Lithuania. Latgale was also touched by repressions against the Poles.

The French Revolution gave impetus to the development of nationalism as well. The nationalism had two main directions. One was the state or civic nationalism supported by the ruling elite of a country and the second was the national or ethnic nationalism, kindled by the communities living in a certain state and directed against the rulers of the state.[37]

Second ideological current of the 19th century that contributed a threat to the existing order was the socialism. Socialism, the same as nationalism, was a collective creed. It spoke against exploitation and oppressors not only to favour an individual, but in the interests of the society as whole.[38] The existing order was attacked by anarchism, which imaginatively speaking "grew up besides the socialism in its childhood, but having grown up, could not get along with anyone".[39]

Reforms in the Baltic furthered the development of education and national self-confidence at the same time. Combined with deprivation of political right, unresolved agrarian situation and dire work conditions in factories it created an explosive situation that came into effect in the revolution of 1905. The situation was even

[37] Deivis, N. (1996). *Europe a History*, 1996 = Deivis, N. (2009). *Eiropas vesture,* p. 825

[38] Ibid, p. 846

[39] Ibid*,* p. 852

more worsened by the Russo–Japanese war (1904–1905) and the defeat of Russia in it.

It is impossible to detail in this article all those historical circumstances that led to the collapse of empires after the First World War, but the concept of the article is matched by a fact that those empires with full (Russia) or partial (Austro–Hungarian, Germany) absolute monarchy fell, but states with a republican system (France, USA) or nominal monarchy (Great Britain) were victorious.

5. The Republic of Latvia (1918–1940)

The Republic of Latvia, proclaimed on November 18, 1918 inherited many problems that constituted a serious threat both to the new states internal and outward security. National tension still existed in Latvia, especially regarding the privileged German minority and the agrarian situation was unresolved with still about half of the land being in the hands of German land nobility. Leftism was popular among the populace and was supported by Soviet Russia in various ways, even by sending armed combatant groups into Latvia.

Most of the problems were solved successfully by the Latvian state. One of the first must be mentioned the successful solution to the problem of citizenship. The Law on citizenship from 1919 defined, that all previous citizens of the Russian Empire that live in the territory of Latvia or originate from regions included in the territory of Latvia without regard to nationality or religion are to become citizens. State system in the Republic of Latvia was established by electing the National (Constitutional) Assembly in democratic elections where both sexes participated. 85% of those having the right to vote participated in the elections of the Constitutional

Assembly and 57 polls were introduced. There was no doubt that the Constitutional Assembly expressed the will of the Latvian nation.[40] Besides developing the fundamental law of the state – the Satversme –, the Constitutional Assembly had a second task, to ensure that the land belongs to those that cultivate it.[41]

To be able to start the confiscation of land the state had to at first prove, that Baltic–German nobility had acquired those lands illegally. The Republic of Latvia did that.[42] The agrarian reform in Latvia was a radical one and it spoiled relations with the previously privileged Baltic–German nobility, but on the other hand made it possible for a stable middle class to emerge. This diminished the influence of the left radical ideas and favoured interior stability and safety in Latvia. The volunteer paramilitary organization "Aizsargi" had an undeniable importance in ensuring interior stability and security especially during the first years of the new state. The "Regulations about divisions of "Aizsargi" in civil parishes" issued by the Provisional Government on March 20, 1919 are seen as the beginning of the "Aizsargi" organization. [43] Women also took part in "Aizsargi" organization. First similar organization for women was created in Finnland in 1920. In Latvia in 1923 thoughts were expressed, that "female units with main tasks in sanitary and culture work" should be created as part of "Aizsargi" regiments.[44]

[40] *Latvijas tiesību vēsture* (1914–2000) (2000). Dītriha Andreja Lēbera red. Rīga: Fonds Latvijas Vēsture, p. 160

[41] Šilde, A. (1976). *Latvijas vēsture. 1914–1940*. Stockholm: Daugava, p. 68

[42] Švābe, A. (1930). *Latvijas agrārā reforma. Agrārās reformas likuma desmit gadu atcerei*. Rīga: Zemkopības ministrija

[43] Butulis, I. (2011). *Sveiki, aizsargi! Aizsargu organizācija Latvijas sabiedriski politiskajā dzīvē 1919.–1940. gadā*. Rīga: Jumava, p. 21

[44] Ibid, p. 145

Unfortunately Latvia and other Baltic states proved unable to agree on a joint defence against great powers that became more and more aggressive in late 30ties of the 20th century. The further destiny of Latvia, the same as in the case of other Baltic states was determined by the Molotow–Ribentrop Pact signed on August 23, 1939. The security of Latvia was not benefited by the withdrawal from principles of democracy – the autoritarian regime of Kārlis Ulmanis was established on May 15, 1934. The people, the army and "Aizsargi" organization were summoned to rely on the President and Prime minister (Kārlis Ulmanis fulfilled both posts since 1936) "… because the President sees farther and will be able to give the most appropriate commands".[45] Of course, Latvia could not hope for any military successes against the huge Red Army, but military resistance perhaps could have lightened and hastened the renewal of Latvian state independence, possibly already directly after the Second World War. Resistance would have deprived the USSR and its successor state Russia the chance to picture the soviet occupation as a "voluntary accession". The biggest gain was the upbringing of a patriotic generation that preserved memories of independent Latvia during the long years of occupation. This experience shows the importance of national self-awareness – if it had not been preserved, the renewal of Latvian state independence would not have been possible.

[45] Butulis, I. (2011). *Sveiki, aizsargi! Aizsargu organizācija Latvijas sabiedriski politiskajā dzīvē 1919.–1940. gadā*. Rīga: Jumava, p. 80

6. The lesson taught by Occupation period (1940–1991)

The soviet occupation power was well aware of this and as a result of deportations and forced migration the proportion of Latvians in Latvia in 1989 had dropped to 52 % of the whole population. The interwar period strengthened mostly the ethnic Latvian self-awareness, although not few citizens of Latvia based their patriotism in a national self-consciousness and belonging to a Latvian nation.

After the destruction of Latvian state independence Latvia was not anymore able to assure the security of its citizens. They were exposed to repressions, as the soviet regime repressed, deported, arrested and killed the financial, political and cultural elite of Latvia.[46] During the occupation of Nazi Germany largest part of Latvian Jewish minority was destroyed. The citizens of Latvia against their will and against international conventions were enlisted in the occupying armies and several thousands lost their lives in a hopeless fight against the soviet regime after the renewed occupation of Latvia in 1944/45–1950.

After the renewal of Latvian state independence in 1991, Latvia has become integrated in international institutions – EU and NATO. Its national security is ensured against a military attack, but threats to the economic safety of the country still exist – it is still amenable in terms of power resources and the coming to power of forces threatening to the Latvian state independence is not fully excluded. Economic hardships in Latvia, inability of EU to solve the

[46] Vīksne, R. (2013). Represijas pret Latvijas eliti (1940–1941). *Latvieši un Latvija. II sējums. Valstiskums Latvijā un Latvijas valsts – izcīnītā un zaudētā.* Rīga: Latvijas Zinātņu akadēmija, pp. 385–404

refugee problem, growing threat of radical Islam coupled with a well targeted and purposeful Russian propaganda and the mythos of Latvia as "a failed state" created by this propaganda creates a fruitful soil for populism, noticeable in the whole Western world. In case of Latvia it can have irreversible consequences.

In a modern world security is not imaginable without professional carers for security – special forces, professional anti-terrorism and rapid reaction forces, but still the role of an individual continues rather to grow than diminish. Only individuals can further the prosperity of a state. Coming to power of forces threatening the independence of the country can also be averted only by the choices of citizens themselves.

Conclusion

Safety is a very complex notion, which includes the safety of an individual, of a community and in modern times – the safety and security of a state.

Since the Reformation in the 16th century the convictions of individuals acquire more and more importance. The fight for the trust of the people began and was conducted both by clergy and by secret agents that can be seen as the predecessors of modern intelligence services. The role of education and science increased.

The dissolution of the Livonia in 1561 shows that a state (or confederation as in the case of Livonia) can be brought to a dissolution through untimely reforms, existence of a gap between the groups of inhabitants and low morals. Military defeats are only the visible results of these factors.

After the French Revolution in Europe the role of citizens in ensuring the security of their state gained more importance. Those states where reforms were delayed and citizen's rights restricted were threatened by revolutionary convulsions. Latvia experienced such in 1905.

During the democratic period from 1918 to 1934 the Latvian state promoted the equality of its citizens and gave them chance to participate in the forming of the state and ensuring its security. Although successful economic reforms ensured the stability of the country, the stepping back from democratic values and relying on the foresight of one single leader contributed to the destruction of the state.

Lessons learned from the past have not lost their importance even today, when the fight is mainly led to win the minds of the people.

References

Ābers, B. (1940). *Latvijas tiesību vēsture.* Pēc doc. B. Ābers 1938/39. lekcijām. Rokraksta vietā

Atskaņu hronika (1998) = *Livländische Reimchronik* (1998). No vidusaugšvācu val. atdzejojis V. Bisinieks. Ē. Mugurēviča priekšvārds, Ē. Mugurēviča un K. Kļaviņa komentāri. Rīga: Zinātne

Butulis, I. (2011). *Sveiki, aizsargi! Aizsargu organizācija Latvijas sabiedriski politiskajā dzīvē 1919.–1940. gadā*. Rīga: Jumava

Deivis, N. (1996). *Europe a History*, 1996 = Deivis, N. (2009) *Eiropas vēsture*. Rīga: Jumava

Eihmane, E. (2012). Rīgas arhibīskapa un Vācu ordeņa cīņas par varu viduslaiku Livonijā. Rīga: LU Akadēmiskais apgāds

Henricus Lettus (2003). *The chronicle of Henry of Livonia*. Translated with a new introduction and notes by James A. Brundage. New York: Columbia University Press. Edition. *Indriķa hronika* (1993) No latīņu val. tulk. Ā. Feldhūns; Ē. Mugurēviča priekšvārds un komentāri. Rīga: Zinātne

Jakovļeva, M. (2004). Kurzemes hercogistes militārā reforma un hercoga Jēkaba mēģinājumi to reformēt XVII gadsimta vidū. *Latvijas Kara muzeja gadagrāmata, V*. Rīga: Latvijas Kara muzejs, pp. 9–20

Jakovļeva, M. (2013). Valstiskums Latvijas teritorijā agrajos jaunajos laikos: Kurzemes un Zemgales hercogistē. *Latvieši un Latvija. II sējums. Valstiskums Latvijā un Latvijas valsts – izcīnītā un zaudētā.* Rīga: Latvijas Zinātņu akadēmija, pp. 121–149

Levāns, A. (2013). Politiskās organizācijas modeļi viduslaiku Livonijā 13.–16. gadsimtā: manifestācijas un leģitimācijas formas. *Latvieši un Latvija. II sējums. Valstiskums Latvijā un Latvijas valsts – izcīnītā un zaudētā.* Rīga: Latvijas Zinātņu akadēmija, pp. 52–76

Latvijas tiesību vēsture (1914–2000) (2000). Dītriha Andreja Lēbera red. Rīga: Fonds Latvijas Vēsture

Rusovs, B. (1926). Livonijas Kronika. Ed. Veispala tulkojums. Rīga: Valters un Rapa. Retrieved from https://www.historia.lv/biblioteka/baltazara-rusova-livonijas-hronika

Stikāne, V. (2001). Kuršu tiesības jeb Kuršu un zemgaļu zemnieku tiesības. Retrieved from https://www.historia.lv/dokumenti/kursu-tiesibas-jeb-kursu-un-zemgalu-zemnieku-tiesibas-teksts-lejasvacu-valoda-un-tulkojum

Šilde, A. (1976). *Latvijas vēsture. 1914–1940*. Stockholm: Daugava

Švābe, A. (1930). *Latvijas agrārā reforma. Agrārās reformas likuma desmit gadu atcerei*. Rīga: Zemkopības ministrija

Tēraudkalns, V. (2017). Reformācija starp mītiem un vēsturi. *Ceļš*. Nr. 68., pp. 59–85

Vīksne, R. (2013). Represijas pret Latvijas eliti (1940–1941)*. Latvieši un Latvija. II sējums. Valstiskums Latvijā un Latvijas valsts – izcīnītā un zaudētā.* Rīga: Latvijas Zinātņu akadēmija, pp. 385–404

Vippers, R. (1930). *Jauno laiku vesture. 1. daļa. Atradumu reformācijas un reliģisko karu laikmets*: Latvijas Universitātē lasītais kurss. Tulk. I. Alksne un M. Rutmane, rediģējis M. Stepermanis. Rīga: Latvijas Universitāte

Zemītis, G. (2010). Komunikācija Latvijā 12. gadsimta beigās un 13. gadsimta sākumā pēc Indriķa Livonijas hronikas ziņām*. Biznesa augstskolas Turība Zinātniskie raksti Acta Prosperitatis Nr. 1.* Komunikācija publiskajā telpā. Rīga: Biznesa augstskola Turība

Latgaļu tiesības jeb Rīgas arhibīskapijas zemnieku tiesības. Retrieved from https://www.historia.lv/dokumenti/latgalu-tiesibas-jeb-rigas-arhibiskapijas-zemnieku-tiesibas-teksts-lejasvacu-valoda-un

Lībiešu–igauņu tiesības jeb Livonijas zemnieku tiesības. Retrieved from https://www.historia.lv/dokumenti/libiesu-igaunu-tiesibas-jeb-livonijas-zemnieku-tiesibas-teksts-lejasvacu-valoda-un

About the Author

Guntis Zemītis is a historian, archaeologist, *Dr.hist.,* leading researcher at the Institute of the History of Latvia at the University of Latvia and Professor at the Turiba University.

THE BASICS OF SECURITY THEORY

Leonīds Makans

Introduction

The awareness of human security and securitability, which as a political notion has been globally known for the past 30 years, has increasingly gained its recognition in Latvia since 2003. Today its strengthening has already become as one of the daily tasks and has been reflected in the law "On National development plan of Latvia for 2014–2020 as one of the state development priorities".[47]

As a consequence, there is an increasing number of those various security providers who are tasked with forming the kind of environment, which would build a sense of security in each member of the society and provide due quality of life.

This article addresses students, who acquire the knowledge needed for lower and middle-level officials of state and municipal institutions as well as for security experts of commercial companies or managers of security services. It addresses the key theoretical notions of security and the manifestations of security issues in the lives of individuals, their collectives, society and the state as a whole.

1. The notion of security and its key manifestations

Notions like "safe", "security" are used daily for describing a state or conditions when something is not unsafe, threatened, something that is protected against accidents, mistakes, damage.

[47] Par Latvijas Nacionālo attīstības plānu 2014.–2020. gadam. Pieņemts: 20.12.2012. *Latvijas Vēstnesis*, Nr. 6 (4812), 09.01.2013.

Speaking of something that is reliable and trustworthy or representing a general quality: safe traffic, safety belt, labour safety, a fireproof locker, reliable news, reliable data, state security, et al.

Security and its varied manifestations have an important role in the life of individuals as well as for groups and other collective bodies, for families, various state and non-governmental organizations, society as a whole and also for the whole country. Each person treasures his/her life, health, the required means of subsistence and daily items, favourable conditions for procreation. In a developed society human existence is safeguarded by various social, economic, technical, ecological and biological systems. Their level of existence, operation and development affects the possibility of human existence itself.

Therefore, the theoretical aspects of security should be viewed in correlation with the theoretical aspects of economic, social and technical systems. It should be noted that the level of security at an individual, family, local community, state and non-governmental organizations, society in general as well as national security level depends on a number of social, economic and technical phenomena. The fundamental theoretical substantiation of the development of socio-economic systems, in its own turn, includes also security theory.

The degree of security of each socio-economic system is mainly determined by life expectancy and quality of life of its population. A longer life expectancy and higher quality of life testify of the security of the respective socio-economic system and vice versa: a shorter life expectancy and lower quality of life point to a social strain and insecurity of that system. Socio-economic systems and the condition of their security also form the basis of national security, the goal of which is to safeguard political rights and freedoms of the population and a sound development of personalities and society as a whole.

All other types of security, including military, criminal security as well as individual and collective security are derived from national security interests and its formative elements. This means that a security model possesses not only a definite structure but also that its constituent elements have a hierarchical nature (mutual subordination) depending on their importance for achieving the overall national security goals.

A security system is not a passive construct of a solely defensive nature. It must be active, targeted at the assessment of an object of threat in order to learn its weaknesses and to predict possible targets of a subject of a threat.

One should distinguish between general and specialised aspects of security theory. The former is related to security system as a whole, while the latter is characteristic only of separate security elements or their types and directions, like anti-terrorism, anti-corruption programmes, etc. For instance, national security concept serves as the basis for the development of military, crime elimination, environmental protection and other security programmes targeted at maintaining security.[48]

One should also discriminate between the external and the internal scope of national security[49], where the former encompasses global and interstate level, i.e. dangers associated with ecological, epidemiological and natural factors, military threats as well as possibilities of expansion of threats of cultural and moral character. The internal scope mostly involves such threats of economic and

[48] Cilvēka drošumspēja un NAP2020. Retrieved from http://www.pkc.gov.lv/lv/valsts-attistibas-planosana/nacionalais-attistibas-plans/cilveka-drosumspeja-un-nap2020

[49] Latvijas platforma attīstības sadarbībai (2018). Cilvēkdrošības pamatjēdzieni. Retrieved from http://lapas.lv/aktualie-jautajumi/cilvekdrosiba/cilvekdrosibas-pamatjedzieni/

political nature as penetration of criminal structures in the market economy relations, threats of coup d'état, the threat of terrorism, emergency situations related to biological and technical character, and serious human rights violations.

The national scope manifests itself at various levels: international/inter-state, state, regional, organizational, professional and personal. The scope of security manifestation areas can be extremely broad: state, social, technological, ecological, criminal, et al.

The most essential notion of security theory is a threat, which can be of a highly varied nature. They are normally categorised by their origin: natural disasters (geophysical – earthquakes, landslides; hydrological – inundation, flood, ice jams; meteorological – rainfall, hail, snow-drifts, storms, whirlwinds); climatological – extreme cold or heat, black frost, drought, forest and peat bog fires; biological – epidemic, epizootic, and epitopic diseases; cosmic – fall of meteorites, geomagnetic storms; anthropogenic, or man-made threats – technogenic catastrophes, resulting from leaks of chemical, radioactive and biological substances, as well as from fire hazards in buildings and edifices, explosions, ruptures of dams and other hydro-technical installations, damaged electrical grids, breakdown of utility networks, collapse of buildings and edifices or transport collisions. They may also result from public disturbances, terrorist acts and domestic unrest, the possibility of which depends on the degree and intensity of social tension in a particular country, region, specific segment of society, et al.

Taking into account the aforementioned description one can argue that dangers or threats should be understood as a totality of conditions and factors, which disrupt normal existence and development of persons or society.

In order to clarify the contents of threats, one must be aware of the disruptive conditions and factors in place and the progression of threat impact. The threat impact and its progression must be viewed in statistics and dynamics. Statistics singles out the source of a threat – its subject and threatened assets – its object, while in dynamics, in addition to a threatened object and a subject, also singles out the target of subject's impact, the process of impact and its results.

Taking into account the diversity of threat subjects and the distinctly different properties of objects and for the purposes of facilitating the understanding of the diverse threat progression, they can be classified on the basis of various criteria.

One of such classification options stipulates division of all threats into 6 groups on the basis of the following criteria:

1) the nature of threat subject;
2) the nature of object;
3) the nature of the means of threat impact;
4) the nature of the target of threat subject;
5) the type of threat impact;
6) the nature of the result of threat impact.

Based on necessity, each of these groups can be divided into subgroups according to separate types of threat.[50]

Thus, the first group can comprise the aforementioned threats stemming from natural forces, technological and social environment, while the last ones can include those related to threats of a political nature or those, which exist in the areas of state institution activity,

[50] Civilās aizsardzības un katastrofas pārvaldīšanas likums. Pieņemts: 05.05.2016. *Latvijas Vēstnesis*, Nr. 100 (5672), 25.05.2016.

economy or spiritual life of society or those stemming from a specific professional activity or behaviour of individuals.

Upon necessity, all the listed threats can be divided even in smaller subgroups. The division would be based on such criteria as, for instance, development of a threat over a period of time: slow or fast developing threats; the eventual destructive power and damage in the course of a threat: substantial, average, insignificant.

The threats of the second group can be divided according to such characteristics as capacity or lack of capacity to reflect a threat in an adequate manner; capacity to perceive a threat actively, neutrally, passively; awareness of the degree of a threat: good, poor, not aware; capacity to eliminate a threat: complete, partial, incapable; readiness to react to a threat: complete, partial, non-existent; the degree of awareness of the consequences: complete, partial, unaware.

For the degree of threat to an object: real or imagined threat; the level of experience dealing with an object: known, dealt with before and resolved (typical) or unknown, unexplored (specific) threat, et al.

Threats of the third group can be divided into simple (single means of impact) and complex (a simultaneous integrated impact by various means), as well as preventable and unavoidable.

Spontaneous and planned threats are included in the fourth group. Such threats could be targeted against an individual, a group of people as well as some particular part of society. In the latter case, threats can manifest themselves locally, regionally and generally. A threat can be targeted against a single or several objects, i.e. it is a single or multi-target threat.

Threats of the fifth group can be either direct or indirect, permanent or recurrent.

Threats of the sixth group are divided into permissible (if the damage sustained is restorable) and impermissible (catastrophic), when the sustained damage cannot be restored and as a result, the damaged object ceases to exist.

The examined notions, terms and definitions for the basic categories of security theory. One must bear in mind that their interpretation is not absolute, it can be used in a generalised way and can be adapted, taking into account the specifics of a particular area of security. The contents of notions and categories of security theory may vary depending on the area of applicability and position of an interpreter. For instance, the criminological interpretation of the notion of security will differ from the forensic and criminal procedural interpretation. It would also be interpreted completely different by psychologists.

The differences in the interpretation of the security notion can manifest themselves also in such areas of security as personal security or organizational security. Moreover, there will be differences of interpretation depending on the profile of an organization. There is also a possibility for an objective and subjective interpretation of the notion of security.

2. Security of power

Security of power is one of the key elements of national security. Based on the legal understanding of a democratic constitutional country, the main task of a state and its executive power is safeguarding the constitutionally guaranteed needs and interests of society as a whole. The state power enforced in such a country is characterised by manifestations of a constitutional state and democracy: conformity with the principle of justice; the division of power; respect for the fundamental human rights; power of the court of law; freedom of active and passive right to vote; freedom to acquire political power; democratic engagement and control over the decision-making process; transparency of the decision-making process; the rights of minorities; the rule of majority.

Each of the listed manifestations is essential in a democratic, constitutional state and their enforcement testifies that the state power carried out in a country can be considered secure, i.e. the kind of power whose main function is to satisfy the needs of society as a whole, not just those belonging to a separate, closed group. A power which does not meet these criteria is considered deformed and dangerous for society.

Absolute power does not exist in practice. Social inequality always creates difficulties, addiction to power, violence, et al. by using all repressive means available to the state power. Their use does not always signals of state power deformation since in the majority of cases some use of measures of compulsion is completely justifiable. However, one can agree to the views expressed in the literature that a state with the instruments and policy at its disposal can become not only a person's ally but also a threat or a source of the threat.[51] In a similar manner, an individual or a body of individuals can either strengthen a state or act as a threat against a state, society and fellow-citizens.

The criminalisation of state, lack of multi-party system, lack of clear division of functions between legislative and executive powers are considered as the most characteristic indicators of state

[51] Сухов А. Н. (2002). Социальная психология безопасности: учебное пособие для студ. высш. учеб. заведений. М: Издательский центр "Академия";

Buzan, B. (1991). People, States and Fear. An Agenda for International Security Studies in the Post-Cold War Era. London: Harvester Wheatsheaf deformation. One can also name such indicators as a weakening of opposition, the existence of double standards, lack of openness, human rights abuses, ignoring of national security interests and others.

Depending on the specifics of one or another country, the forms of state power deformation and their manifestations can differ. For instance, joint characteristic traits of all post-socialist countries include subordination of state interests and the interests of society as a whole to the pecuniary interests of individual groups, corruption, excessive bureaucratisation of state power, et al. The notion of state power is viewed in a generalised way without specifying the functions, authority and interaction of individual institutions.

In order to overcome state power deformation and to develop a safe power for the society, it is necessary to implement the principles of safe power formation: improvement of the power formation mechanism, optimisation of the election system, improvement of candidate selection procedure, precluding criminally engaged, mentally ill, incompetent people from state power structures improvement of evaluation and training of civil servants; formation of a national political elite, et al. In order to safeguard the control over the action of state power, the role of non-governmental organizations should also be simultaneously strengthened.

3. Social security

Social security is another essential element of national security, which views the condition of state economic, public institutions and social groups in their totality.

The level of social security is characterised by social tension. The higher the tension, the lower the level of social security and vice versa.

Social tension is understood as a totality of indications (syndromes), which characterise physiological, psychological and social adaptability (adaptation or disadaptation) changes of various groups of society reacting to various difficulties of daily life, e.g. price increase, lowering standard of living, unemployment and other factors.

Manifestations of social tension are different: a dramatic rise in popular dissatisfaction, conflicts in society, mistrust towards state institutions, worsening of the demographic situation, et al. They go hand in hand with compensating reactions: the rise of aggressiveness, search for enemies, hope for a "strong leader" and a miracle, increasing interest in mysticism. The level of tension can also be affected by ecological, technological and epidemiological factors.

The loss of physiological capacity to adapt (disadaptation) to difficulties and social changes by a certain part of the population is considered to be one of the causes of social tension. It manifests itself as a decreasing birth rate, rising mortality and increase of serious illnesses.

Another reason should be sought in psychological disadaptation, which is reflected in various mental phenomena – unfounded anxiety compensated by aggressiveness or apathy.

Psychological disadaptation is another reason for social tension. It is reflected as a conscious conflict-orientated behaviour of a certain strata of society. It is characterised by a highly politicised behaviour, dissatisfaction, pessimism, migration, emigration, engagement in criminal activity.

Social tension can develop both: spontaneously and in an organised manner inspired by opposition representatives and criminal structures.

It can be either destructive with devastating effects to state power, economy, society, or constructive – tended towards overcoming of difficulties and thus having a mobilising role. Therefore, social tension is not only a barometer of security level but also a strong and necessary source of motivation for a society.

One can distinguish several levels of the development of social tension: low, medium and high. The low level of tension does not substantially affect the society, the medium level already poses a noticeable impact, while the high level of tension can disorganise work of social and public institutions.[52]

The levels of social tension are determined on the basis of such criteria as the level of dissatisfaction of the population and its nature (economic or political), the authority of state power and the loyalty of the institutions of executive power to it, the impact of media and criminality on social tension as well as the level of unity of the political opposition – the existence programmes of action, presence of a leader (or lack of them), etc. When assessing social tension one must also distinguish its origin, i.e. if it has a general nature similar to the whole country/a certain region or a local nature, which may have embedded causes for further difficulties, e.g. a conflict situation in a factory, in a separate quarter of a town, etc.

Along with such social tension inducing factors as natural phenomena, technological, ecological and epidemiological causes, social tension is also caused by social factors, which represent the most complicated challenge. These factors also include issues like the effectiveness of public administration, the overall economic

[52] The levels of social tension are established on the basis of specially developed indexes. Their detailed description can be found in the Social Psychology study course

situation and the standard of living of the population. In the context of these factors one could also name such tension-aggravating phenomena as the sense of unpredictability among the population and its level of welfare which should be viewed in terms of access to the goods of primary necessity, prices on services vs. income, as well as the level of unemployment.

Based on the presence of those factors, it is possible to establish specific sources or hotbeds of the rise of social tension. The hotbeds of social tension can exist within specific groups of population: among retired people, students, lower income employees of public institutions. They can also be inhabitants of specific streets, buildings, boroughs who are, for instance, dissatisfied with turning off of heat or some accident of a localised nature. The criminogenic situation in specific areas (towns, boroughs) can also serve as hotbeds of social tension.

The form of manifestation of social tension consequences can be varied. In this regard, social and demographic phenomena are named most often. They include: lowering of birth rate, rising mortality, lowering of life expectancy; peculiarities of the criminogenic situation: an increase of specific types of crime, distinctive changes in the criminal environment; psychological peculiarities of specific strata of society: anxiety, depression, aggression or panic as well as the peculiarities of people's behaviour in general: public picketing and rallying, demonstrations, hunger strikes, industrial action (strikes), demonstrative cases of suicide.

From the point of view of applying various degrees of security measures, all of the listed forms of social tension can be equally dangerous. For instance, the danger of mass depression shows itself in the way that it can paralyse various forms of social life: people do not want to join activities of political parties, do not participate in elections, etc. whereas the dangers of picketing, demonstrations or strikes will be characterised by the unpredictability of actions of masses of people.

Factors causing social tension and defining its level can be linked not only with domestic problems of a country but also to outside conditions: the global economic situation, ecological problems, international security, etc.

Therefore one can argue that social tension significantly affects the level of security. Knowledge about its roots and manifestations makes implementation of required security actions considerably easier.

Social conflicts

Social tension can result in social conflicts. In the daily life, the notion of "conflict" is usually used in a simplified way, understanding it as substantial differences, an argument, a fight, etc. From the perspective of the defined security levels and in the interests of security theory conflict must be viewed as a socio-psychological phenomenon.

Although social psychology includes various approaches[53] to clarifying the notion of conflict, one should note the key characteristics of a conflict: differences or discrepancies of human roles, motives, goals, values and interests; counteractions of the carriers (subjects) of these differences and discrepancies targeted at damaging the opposing party; expression of negative feelings and emotions between subjects engaged in a conflict.

[53] For detailed information on conflicts, see V. Semenkova (2006). Drošības psiholoģija. Uzņēmumu drošība. Rīga: Biznesa augstskola Turība, pp. 233–285; Pikeringa Pega (2000). Strīdi, nesaskaņas konflikti: kā izvairīties no kļūdām to risināšanā un sekmīgi pārvarēt domstarpības. Rīga: Jāņa Rozes apgāds, p. 116

In the security context, one should pay attention to the parties (participants) engaged in a conflict, its spread, the subject matter of a conflict as well as to the perception of the engaged parties of their own motives, values, possibilities of reaching their goals and those of their opponent. The thoughts of each participant on how the opponent perceives the other party and the environment where the conflict takes place are highly important. Parties to the conflict can be individuals, social groups, states or their associations.

According to the spread of the conflict, conflicts are divided into global, regional, local and interpersonal.

For the purpose of assessing various conflicts, it is important to pay attention to the areas of conflict' origin and progression (politics, economy, society, et al.); to the time and place of conflict origin and progression; to the pretext and conditions of the collision; to frequency of collisions (episodic, regular, cyclic conflicts); to conflict progression in time (short-term and prolonged conflicts); to the tools used by participants in reaching their goals (disinformation, spreading of rumours, blackmail, bribery, et al.); to the verbal (non-verbal) form of manifestation, which can be either open or hidden.

Functions (tasks, significance) of a conflict are revealed by its final outcome. A function of a destructive conflict can manifest itself in the form of an emotional tension, mental trauma, violation of law, and military clashes. Conversely, a creative or constructive function helps to strengthen the positive vectors of communication, pushes towards abiding by the norms of law, and improves the psychological atmosphere. A gnostic or diagnostic function is also a possibility, allowing to survey and understand causes of a conflict and motives of subject actions.

It is important to be aware that any conflict originates and progresses in time, thus forming a process. The principal pattern of conflict origination and progression involves a pre-conflict situation, a stage of mutual impact of conflicting parties and conflict resolution.

During the first stage, one observes escalation of relations, a possibility of demonstration of distinctly formal relations, stratification and grouping of people, etc. The interrelation between the conflicting parties can proceed in the form of avoidance of confrontation, also as conflict resolution or as a "fight until a complete victory". Taking into account the extreme diversity of conflict situations, other versions of conflict progression are also possible. Therefore, being aware of general regularities of conflict origination and progression, one should study their specifics in each separate case. This serves the purpose of raising the capacity of conflict prediction/forecasting, conflict prevention or finding other solution.

When studying conflicts for practical purposes one usually pays attention to the following conflicts: socio-political and ethnic-political conflicts; ethnic conflicts; conflicts in the field of administration; conflicts in the fields of production, trade and services; conflicts in scientific institutions; conflicts in the military area; conflicts at detention facilities; family conflicts.

The classification of conflicts provided in this work should not be viewed as absolute as they can be different in each specific situation and under its specific circumstances.

4. Criminal security

Criminality is one of the factors, which can tangibly affect security situation in a country. First of all, it decreases the attractiveness of a country from the point of view of the attraction of foreign investment. It also destabilises society, it can create hotbeds of tension and in individual cases, it can lead to armed confrontation and a number of other negative effects. The notion of criminality is normally understood as “the existence of crime, delinquency.”[54]

However, this explanation does not provide a complete picture of this notion. One would argue that the notion of criminality should also include the criminal environment itself, the conditions of its existence and committed crimes. This notion must also include a description of a criminal activity in the context of criminal law, criminology, forensics and criminal investigation.

From the point of view of the security theory, criminality should be viewed not only in the aforementioned legal, crime disclosure and investigative context but also from a social perspective: as a type of public activity, which reflects the nature of cultural, economic, state, non-governmental institution relations. It should also reflect the dynamics and structure of linkage between a political regime and criminality as well as the most drastic manifestation of the deformity of public relations.

5. Emergency or crisis situations

When addressing the key notions of security theory, we already touched upon the diverse nature of threats and the prospective damage and consequences of their impact, which can manifest themselves as a crisis (emergency) situation.

Crisis or emergency situations should be understood as a dangerous, complicated and difficult transition period in the life of a society or something completely unusual, unexpected, unprecedented and novel.[55]

[54] Latviešu literārās valodas vārdnīca. Retrieved from http://www.tezaurs.lv/llvv/

[55] Ibid

Crises can overlap with one another and can manifest themselves in the most diverse forms of social tension. Depending on the level of tension in a society, today issues related to overcoming crisis situations at various levels affect not only social psychology experts and the various security providers, but almost every inhabitant of a country.

Natural disasters caused by climate change and resulting from global warming is a potential topical contemporary source of crisis. One should also mention the various infectious diseases, which are spreading inter-regionally. Over the past years, terrorism has been assuming an increasingly widespread character. A crisis situation can also occur during a sports event, music performance and during political events. In all cases of crisis, it is possible to encounter threat related mass phenomena as crowds, rumours and post-traumatic stress.

Crisis situations are often linked with a gathering of crowds whose psychological peculiarities of behaviour contains threats to their participants as well as to bystanders and to those in charge of maintaining security and order. Threats embedded in a crowd can be aggravated by fire hazards, floods, epidemics and other consequences.

A crowd is viewed as a disorganised group of people who are in contact with one another. Crowd members are characterised by conformism, the unity of action and emotionality.

A crowd has a strong psychological influence on its individual members, who, influenced by a feeling of anonymity, lose the sense of personal responsibility and, at the same time, gain in self-confidence. A crowd instigates “infection” of an individual who is part of it. When in contact with other members of the crowd who are in a similar emotional state (anger, fear, joy), the mental state of an individual is intensified. This “infection” or the sense of being overwhelmed proceeds by means of verbal and non-verbal (gestures, facial expression, etc.) communication.

The effectiveness of a crowd can show itself in various ways, depending on individual and group features of its members. For the sake of comparison, one could mention the different crowd reactions during the Song and Dance Festival, a rock festival, a hockey or a football game or an anti-globalisation rally.

Although a crowd can form itself spontaneously, it is quite often created on purpose, using rumours, threats, blackmail, taking hostages, et al. For instance, rumours as a crowd-forming provocative tool consist of the statement containing false or only partially true information on some event. Rumours are spread by one or more persons and they are orally multiplied to an unknown number of people. In addition to that, psychological devices of influence are also employed.

Inspiring is one of the most widespread of such devices and is used by subjects by means of issuing various statements – rumours, appeals, threats, et al. Inspiring is always verbal and its subjects always act consciously.

Explanation and persuasion are other devices of psychological influence. Whereas inspiration is rooted in blind trust and does not require a logical explanation of the information received, the opposite is required in the case of explanation and persuasion. Acceptance of information is achieved through intellectual influence, by appealing to logic and common sense.

When assessing the devices of psychological influence, one should bear in mind that they are not always linked with verbal transmission of information. Significant influence can be achieved by a definite level of noise, sound frequency, and individual rhythmic exclamations.

Imitation is another device for influencing and forming crowd activities. The effect of imitation lies in the condition that the behaviour of an individual or a group not only is understood and accepted but is also multiplied.

It should be noted that joining the crowd results in drastic changes in human behaviour. This is linked with levelling of individual traits of participants: all people think and experience the same. The intellectual level of an individual falls and while being part of a crowd an individual is capable of committing any violent act, which under normal circumstances would have been unimaginable.

A crowd has a leader. Understanding the role of a leader is vital from a security perspective. There is a view that relations between an individual in the crowd and a leader of a crowd are similar to a child and father relationship in a family. Each member of a crowd identifies himself with a leader. As a result, a crowd gains homogeneity and unity. There are several types of leader – leaders loved by a crowd, leaders feared by a crowd and leaders whose ideals are shared by a crowd. From the perspective of a leader, his/her relations with a crowd are similar to child's relations with parents. Children are afraid to lose parents.

While observing crowd formation and its action, one can distinguish simple, expressive, conventional, and active crowds. The simple crowd involves the gathering of people for the purpose of gaining information on events or phenomena the people who gathered had witnessed by accident. This kind of crowd often gathers at traffic accident sites or due to somebody's strange or erratic behaviour, et al. Despite the fact that this swarming can cause inconvenience to some daily chore, this type of crowd is not usually perceived as a source of a serious threat. However, under certain circumstances, this crowd can turn into an active, aggressive crowd.

The expressive crowd involves the gathering of people for the purpose of demonstrating their emotions and feelings, e.g., at concerts, public rallies, festive demonstrations or funerals. The degree of threat of such a crowd should be estimated depending on the type of event in question.

A conventional crowd is formed by individuals who have gathered for an event and behave according to the accepted norms. This crowd can be formed by fans of a sports team, whose behaviour sometimes causes a real threat to the public order and safety. In many cases a considerable part of fans are people who are not interested in sports, they are persons who feel animosity towards an opponent, most often towards hosts.

The active crowd is a group of people, whose shared emotions and verbal expression of wishes transforms into action. This crowd is sometimes divided into subtypes: a crowd in search of a rescue, a crowd of misers and an aggressive crowd. In the first case, the crowd is panicking, there is an uncontrollable fearful reaction to a real or imagined threat. Panic can break out in places of people's regular gathering due to fire, natural disasters, terror acts and other reasons. Random, disorganised groups of people are more susceptible to panic.

The crowd of misers can form itself during some big sales events, at the stadium or other entertainment venue box offices selling a limited amount of tickets, etc.

The aggressive crowd is often formed by groups of people who, in order to express dissatisfaction, engage themselves in violence, arson and other illegal actions. They can be hostile antisocial informal groups, football fans, et al. In other cases, members of such groups could be organisers of social protests, e.g., opponents of globalisation, participants of unsanctioned rallies. In such instances, a crowd is formed in a conscious, professional manner and with a definite goal.

Persons who are part of a crowd are divided as follows: organisers – persons who work out scenarios, plan and determine optimum time, place and pretext for organising violent actions; initiators who engage in active incitement and divide roles among people, and spread rumours. They could be the persons aiming at a leader role; active participants – perpetrators of violence, they form the main force of a crowd; conflicting persons, who are subordinated to the active participants of violence in order to settle scores with someone anonymously, to let off steam, engage in fighting. They can often be psychopaths and drug addicts; persons who have participated in violence as companions in a delusional good faith (mistakenly perceiving the causes of a situation, mistaken sense of justice, impact of rumours); emotionally unstable persons who easily succumb to the mood of a crowd; the inquisitive – people, who observe violence but do not engage. However, their presence intensifies agitation of other participants; accompanying persons – those who have become participants due to a threat.

Group excess/violence, as well as the emergence of crises and their progression, takes place in several stages. During the pre-crisis stage, one can observe aggravation of the situation, an increase of social tension, accumulation of dissatisfaction, which requires just a smallest trigger for further escalation. The commencing of this stage can be signalled by a drastic tendency of social stratification, circulation of disturbing news, rumours, negative views and moods, dissatisfaction with actions of the authorities, a decreasing standard of living and other factors.

The crises stage itself, which is triggered by organisers and initiators finding a pretext and using it for further action. They usually select an event, which from a psychological point of view can be interpreted as justifiable for the violent actions of its participants. An event, which would grant those actions an illusion of justice and would allow drawing in the violent actions maximum amount of people. In cases of group violence, demands to authorities usually are expressed from a position of strength asking for immediate execution and trying to attract public attention. There are efforts to create onerous conditions for the operation of law enforcement authorities. There is a possibility for further acts of violence and physically destructive action.

The third post-crisis stage develops after the dissolution of escalation. After the crisis is over the situation does not normalise immediately. There is still a window of opportunity for rumours, dissatisfaction and other negative phenomena, thus inherently containing a possibility for a crisis relapse. The situation can also be aggravated by the consequences of catastrophes, fires, etc. These events cause psychological reactions, possibly leading to pathological changes in the human body, also called post-traumatic stress syndrome. Therefore, one of the main tasks during the post-crisis stage involves providing psychological, medical and other assistance to the victims. This assistance must be provided by services engaged in dealing with the consequences of the crisis. One should try to provide assistance as soon as possible, by trying not to change the conditions of the social environment and by minimising the negative consequences of hospitalisation.

When providing assistance to a person in a post-stress situation, he/she should be treated like a regular person and not as a patient. Assistance must be simple: the victim should be taken away from the source of the threat and the services must provide the victim with food, rest, and sense of security. Victim’s story should be heard out as well and with care. This general insight into origins and development of a crisis situation (extreme crisis) provides a possibility to establish additional study directions, as well as to develop recommendations and methods in order to prevent such situations or to relieve their possible consequences.[56]

6. Societal security

Societal security is one of the main types of national security. While studying it, attention should be paid to its social and civic aspects and their place and role in national security in general. Addressing national security issues, we already established that the main task of executive authorities of every democratic, constitutional country is to enforce implementation of the needs and interests of the society and every one of its members.

Due to the fact that the state and its structures are formed and paid for by the society consisting of individuals, the society has the right to advance and control actions of the state. It should happen on the basis of the premise that an individual and his/her human rights form the basis of the society.

In order to achieve this goal, national security system and security safeguarding must rely on collective efforts of the society and the state.

Therefore, the national security system should develop on the basis of interconnected, but independent systems: national security and societal security. Their interconnection is determined by the overall national security interests, common legislation of the

[56] For more detailed reading on crowds, see: Pikeringa P. (2000). Strīdi, nesaskaņas konflikti: kā izvairīties no kļūdām to risināšanā un sekmīgi pārvarēt domstarpības. Rīga: Jāņa Rozes apgāds;

Таранов П. С. (2003). Приемы влияния на людей. М: Фаир Пресс; Сухов А. Н. (2002). Социальная психология безопасности: учебное пособие для студ. высш. учеб. заведений. М: Издательский центр “Академия” two systems regulating legal authority, duties and dispute settlement procedure in cases when their interests do not overlap.

The interests of the state and the interests of society may correspond, but they can also be different. A strong system of well-organised institutions safeguarding national security can only become a safety guarantee of the system itself while at the same time distancing itself from the largest part of society and as a result, it can become dangerous. Therefore, the society has an important role to play in monitoring the activities of both: individuals and state institutions responsible for national security.

The societal security system can be formed by individuals, their collective bodies, non-governmental organisations and public self-governance bodies.

Formation of societal, non-governmental security system is multi-dimensional from the point of views of both: area of public life it deals with, as well as from the perspective of its legal and organisational forms.

The most widespread forms include various security guard companies, security services, associations, federations and other similar entities. They can also be joint stock companies, limited liability companies, physical persons who deal with the issues on a private basis, private detectives, consultants, bodyguards, various training programmes at educational institutions, et al.

Despite the seemingly chaotic emergence of such bodies, nevertheless, it exemplifies an increasingly active formation of societal security.

The key tasks of societal security system include control of the state power; oversight of information progress and impact, defence against mental aggression, defence against crime, assessment of state and public projects from the perspective of public interest.

Thus one can argue that simultaneous existence and operation of independent security systems form a balancing mechanism, which protects an individual, society and state from such dangerous manifestations of power as amateurism, malice and incompetence of civil servants that result in higher social tension and increased risks of social crises.

It was already established before that one of the indicators of societal security is the self-organisational ability of people. This depends on the degree of self-confidence and activity of each individual. Therefore, for the purpose of implementing security measures of any level, it is necessary to be aware of some factors, which can affect negatively the development of an individual and the society and as a consequence – also societal security.

Post-traumatic social disorganisation, which is similar to post-traumatic stress syndrome, is considered one of such factors. This phenomenon was first observed and defined in the USA. Its basis is the inability of Vietnam war veterans to adapt to normal life without the help of society.

Post-traumatic social disorganisation develops after traumas, serious illnesses, and prolonged stays in extreme (crisis) conditions. The most typical signs of such disorganisations include irritability, aggressiveness, fearfulness, low level of concentration, lack of belief in future, the sense of insecurity, alcoholism, and drug abuse. Prolonged exposure of a person to an extreme situation and the ability to survive it develops corresponding behavioural models, which can be inherited by next generations.

For instance, the history of the inhabitants of the former USSR, the wars they survived, repressions, emigration, life under a totalitarian regime are to be considered as a traumatic factor, which has substantially affected people’s behavioural pattern. Posing trauma to people is one of the tools for the establishment and running of a totalitarian state, the freedom of personality of people was suppressed by various means of scare tactics. A scared society like a scared person is easier to be manipulated.

The rapid political and economic changes that have taken place over the past years for a large part of society have also been traumatic and personality deforming. People encountered phenomena, which up to one point were alien to them: economic hardship, unemployment, the rapid rise of criminality, the emergence of extremely dangerous and severe types of crime, alcoholism, drug abuse.

Social traumatism and traffic accidents were also on the rise, which can be partially explained by the stress-related decrease of concentration capacity. The instances of suicides rose, including youth suicides. We still come across as dissatisfied, agitated, aggressive people on a daily basis.

One can also see that a significant part of society suffers from an extremely low self-esteem. Many people do not want to take upon themselves problem-solving responsibility, believing that it has to be done by someone else, usually by the state. All failures are explained not by personal mistakes, but by the influence of some outside forces/factors. One can often observe unmotivated and highly distinct subservience to superiors and demonstration of distinct superiority towards subordinates. Deformations are also expressed as a highly simplified world-view, seeing it only in terms of good and evil, with a permanent search for an enemy and with grave suspicions towards everything. Changes in human values is another factor aggravating personality deformation: all means (not just unethical but also criminal and they are justified due to objective economic circumstances) are justified in reaching a goal.

The examples listed above should not be perceived as a criticism of the existing situation, but as information, which helps to predict one or another threat and to implement corresponding security measures in practice. Societal security problems exist at all times because the development of society always faces various difficulties, social conflicts, which it tries to overcome.

From the point of view of security, overcoming these difficulties should be accomplished by employing constructive, legal means, including such means as sanctioned rallies, pickets, strikes, adoption of various declarations, election boycott, et al. However, the legal nature of such actions does not take away anything from the fact that they still retain the inherent character of crowd behaviour and they can turn into unsanctioned actions – blocking of roads, the occupation of administrative buildings and other illegal attempts.

Social conflicts can also be resolved in a destructive manner by employing such means as political, economic, national, religious extremism and terrorism. All of this is extremely dangerous, but over the past years they have been widespread global phenomena.

7. Information security

The term information is understood as news, data, and totality of knowledge. Information has an enormous role – exhaustive information is the basis for solving any problem. Therefore, information security has gained particular importance.

Over the past years, the rapid development of information technologies (IT) has been a characteristic trait, resulting in a global shift from an industrial society to the information society. When addressing the issue of information security, one should touch upon the notion of information space, which is formed by information resources, information exchange (telecommunications) infrastructure, mass information system, IT and services market, linkage with the global open information networks, and the legal regulation of the circulation of information.

An orderly situation in the information space implies that it is accessible to the society and capable of providing a coordinated answer to the interests of people, society and the state. Establishment of such information space, first of all, depends on the policy of the respective country.

Although modern technologies by providing information exchange have already contributed to an extremely fast development of the economy and other public spheres of life, they also bring along several negative phenomena, which require securing information itself and securing people from its negative impact. This is why we can talk about information security, which calls for addressing the following tasks:

1) ensuring the rights of an individual and society to receive information;
2) providing circulation of objective information in the media;
3) fighting attempts to use information and telecommunications for criminal purposes;
4) defending of individuals, society and the state against informative and psychological threats;
5) countering disinformation, rumours and slander.

Information security must be implemented in various areas (politics, economy, state defence, et al.) at different levels (state, regional, organizational, individual). Thus security measures will also be different and adapted to various areas and different levels.

From the point of view of security one must talk about informational threats (dangers) and information security. In the former case, we are talking about a targeted informational impact on a person, society or a state performed by definite political or social actors. The goal of these actions is to deform the development of the targeted state, society, organizations or individuals. An example of such actions is the use of media for the purpose of spreading rumours and libel on rival political forces.

Information security in its own turn should be defined as safeguarding the right of society to obtain objective information while ensuring that confidential information is kept away from outside subjects as well as protecting individuals and society from the exposure to informational and psychological threats.

When speaking about information security one should remember that it is not just about keeping of classified information safe, but also about providing access of all interested parties to truthful, non-classified information. Media has an important role in this regard and is derived from the opportunity of exercising real political freedoms in the country.

Enforcement of information security comprises a set of legal, organisational and technical actions and special measures. Legal actions imply the development of regulatory legal norms related to the circulation of information and its use as well as liability for their breach.

Organisational and technical actions imply running diagnostics against an opportunity of an unauthorised access to protected information and the use of correspondent technical devices to ensure its protection.

Special measures usually involve activities of the police and other law enforcement authorities in order to detect, prevent and investigate crimes against information data systems or crimes committed by making use of such systems.

There can be different types of criminal activity; computer-assisted forgery, inducing damage to electronic data or software, unauthorised access, development and spread of computer viruses, et al.

Criminal offences performed by using information data systems can be different and they can be grouped on the basis of the direction of activity of criminal subjects, e.g.: terrorism, military or industrial espionage, human trafficking, money laundering, etc.

Along with the rapid development of IT, we have encountered a new notion: "information warfare", which implies the use of any action in order to restrict information provisions of the opponent, to distort or to destroy information at opponent's disposal and at the same time: to protect one's own information from similar actions of the enemy.

Psychological war is one of the most widespread directions of this warfare. It shows itself as an attempt to affect the psychology of a society by means of media.

Advertising is one of the most widespread forms of such influence. Successful advertising can stimulate certain actions. Information fragmentation is yet another form of informational aggression. It implies presentation of fragmented information under the circumstances of narrow specialisation, thus preventing to see the complete picture in all its interconnectedness.

Immediate transmission of news also involves information fragmentation, since it is superficial and with a degree of sensationalism, it lacks any elements of analysis. All this increases a chance of manipulation with such information.

Another popular method of informational aggression is interception of information, involving outpacing others in presenting news. This method allows persuading the audience of the objectivity and truthfulness of the author and message carrier.

Media has a particularly important role in information security, since, consciously or not, they can become an instrument of informational aggression. In this context media independence, the existence of independent media in the country, political freedoms of citizens and the lack of censorship are an extremely important provider of information security guarantees.

The right of an individual of access to objective information is a crucial information security indicator in any country. At the same time, it should be taken into consideration that this type of general availability can pose a threat to individuals, groups, organisations and the state as a whole. Therefore, part of information should be protected from unsanctioned access. Therefore, legislation is the main tool of information security of every country. Information is usually divided into unrestricted, and information, which has been classified according to various degrees of security clearance access.

Public relations as an institution of society serves as one of the implementation tools of state information security, ensuring exchange of information between an organisation and the general public.

In most of the cases, institutions of public relations organise their relations with media directly. Their functions include providing media representatives with information of their interest, countering disinformation, et al. This function is usually performed by public relations officials of the respective institutions.

8. Organizational security

Similarly to national security, organizational security is formed by many types of security. It is determined by the extraordinary diversity of organizations. Therefore, in order to gain a better understanding of organizational security, it is advisable to review the basic issues of their security system.

The development of security concepts is one of the most substantial issues related to organizational security. Security concepts consist of a prognosis/forecast of possible internal and external threats and measures for averting them and the projection is based on the assessment of external political, economic and social situation coupled with the assessment of the internal situation of an organization.

The existence of such a sound concept provides an opportunity to develop a plan of security measures on the basis of specific conditions of one or another organization. Sometimes it is due to the lack of a conceptual vision of a security system that deems some security measures ineffective.

In general terms, an organizational security system should envision several types of security, for instance, physical security, technical security, information security, economic security, socio-psychological security, legal security, management security and criminogenic security. Each of these types of security requires the establishment of their external and internal scopes, specific tasks and methods of implementation of security measures.

For instance, the external scope of physical security will involve administrative and production facilities of an organization, its top manager and other senior officials, while the internal scope will include other employees. Tasks related to physical security would include physical guarding of the aforementioned facilities, while the methods of physical defence would include preparation of positioning schemes for security forces, development of movement routes of officials, development of emergency situation information posting schemes for personnel, physical conditioning and training of security guards and other activities.

The external scope of technical security would include, for instance, the degree of wear and tear of equipment, technical means of guarding, transportation, while the internal scope would involve officials and buildings. In this case, the issues in need of resolution include technical guarding of buildings and personnel and safe use of transportation. Methods to be used for accomplishing this task: installation of alarms, video surveillance and fire safety equipment, use of the technical labour safety solutions, training, repair of equipment, simulation of crisis situations.

The external scope of information security would include the issue of the image of an organisation and its top manager, prevention of information leaks from the local computer network and from members of staff, while the internal scope would involve public relations structural unit of the organization, the issue of informing staff members (clearance to access certain levels of information), protection of computer networks, identification of the sources of information leaks recruited by competitors. Issues to be addressed: protection of information. Implementation methods: the creation of a public relations structural unit for working with media, classification of information and introduction of a clearance system, securing of communication equipment against bugging, et al.

In the economic security area, the external scope can be attributed to the solvency of customers, legal obligations, while the internal scope: to the level of staff proficiency. In this case, the main task from a security perspective should be defined in terms of economic efficiency, while its implementation would be possible by assessing the specifics of debtor' legal obligations and including them in a database, by controlling payment deadlines, tariffs and other aspects related to this matter.

In the area of socio-psychological security external security scope will be attributed to the image of an organization, while the internal scope will address the dominating psychological atmosphere in the organization: conflicts, informal groups, groups of risk (people with drinking and/or drug abuse habits, etc., rumours, loyalty of employees). The main task: ensuring the internal stability of an organization. Implementation methods: staff selection procedure, staff evaluation, a survey of public opinion, the introduction of a telephone hotline, studying of socio-psychological phenomena, the introduction of a psychologist position.

The external scope of legal security: contractual issues and the practice debt collection; internal scope: legal service. The main task: legal protection. Methods of implementation: legal training of personnel.

The external scope of management security involves relations with media, state authority, law enforcement authorities and other institutions. The internal scope would touch upon the issues of management strategy, information flow, crisis prevention planning, staff relations work. The main tasks would involve management optimisation measures for daily and crisis situation purposes. The accomplishment of tasks would be achieved by means of raising qualification measures, regular evaluation and staff goal-oriented motivation.

The external scope of criminogenic security is formed by threats posed by the external criminal environment, while the internal scope: by the negative socio-psychological phenomena in the organization itself, negative tendencies in its smaller subgroups, the issue of the impact of criminality. Resultant tasks: prevention of incidents of criminal nature. Methods: prediction/forecasting of conflicts, implementation of measures related to all the listed types of security (physical, technical, information, economic, socio-psychological, legal and management).

This security system model tailored for an abstract organization and offered here has an advisory purpose only. It can be used as a general scheme outlining the main principles of operation and can be used as a model for organizations to follow when implementing their own security systems and taking into account their own specific situation.

Conclusions

Taking into account all the issues addressed in this paper we can define security theory as generalised system conclusions involving various branches of science, which provides the basis for researching and studying the regularities in the area of security related to individuals, their groups, society and the state and on that basis make an informed prediction on eventual threats and their consequences for the purpose of developing measures required for their prevention.

References

Autoru kolektīvs (2006). *Uzņēmumu drošība*. Drošības psiholoģija. Rīga: Biznesa augstskola Turība

Buzan, B. (1991). People, States and Fear. An Agenda for International Security Studies in the Post–Cold War Era. London: Harvester Wheatsheaf

Pikeringa P. (2000). Strīdi, nesaskaņas konflikti: kā izvairīties no kļūdām to risināšanā un sekmīgi pārvarēt domstarpības. Rīga: Jāņa Rozes apgāds

Сухов А. Н. (2002). Социальная психология безопасности: учебное пособие для студ. высш. учеб. заведений. М: Издательский центр “Академия”

Таранов П. С. (2003). Приемы влияния на людей. М: Фаир Пресс

Cilvēka drošumspēja un NAP2020. Retrieved from http://www.pkc.gov.lv/lv/valsts-attistibas-planosana/nacionalais-attistibas-plans/cilveka-drosumspeja-un-nap2020

Latvijas platforma attīstības sadarbībai. (2018). Cilvēkdrošības pamatjēdzieni. Retrieved from http://lapas.lv/aktualie-jautajumi/cilvekdrosiba/cilvekdrosibas-pamatjedzieni/

Latviešu literārās valodas vārdnīca. Retrieved from http://www.tezaurs.lv/llvv/

Civilās aizsardzības un katastrofas pārvaldīšanas likums. Pieņemts 05.05.2016., *Latvijas Vēstnesis*, Nr. 100 (5672), 25.05.2016.

Par Latvijas Nacionālo attīstības plānu 2014.–2020. gadam. Pieņemts 20.12.2012., *Latvijas Vēstnesis*, Nr. 6 (4812), 09.01.2013.

About the Author

Leonīds Makans, *Mg.iur.*
In 1979 graduated Faculty of Law of the State University of Latvia.
From 1990, he worked at the Police Academy of Latvia as an assistant, lecturer, associate professor.
Since 2006 work as Visiting lecturer at the Turiba University.
2010-2011 Associate Professor at the University of Latvia, Faculty of Law. Since 2011 guest lecturer at the Daugavpils University Law Department. More than 30 publications on the issues of combating, crime prevention, and safety issues (including one monography).

SECURITY CONCEPT IN A GLOBAL WORLD

Raimundas Kalesnykas

Introduction

A characteristic feature of the beginning of the XXI century is intense processes of globalisation, embracing all spheres of political, social and economic development and manifesting themselves in all regions of the EU. In the process of globalisation, an EU society of a new type is being formed, with its new typical values and new aspirations, which creates new patterns for lifestyle and is confronted to new problems and searches for solutions to these problems. One of them is creating a secure Europe serving and protecting citizens.[57] Globalisation processes are showing themselves very well in modern Europe. It is quite possible to state that the key feature of globalization in Europe is the fact that an integral European society is being born, which creates and builds on an integral security space, as well as integral spaces for social, economic, political, technological, ecological and information development. From this point of view, we could show the relevance of the research which is related with the analysis of development of integral security space in the EU. Looking forward to a new EU Internal Security Strategy, it can be observed that this strategy not only creates preconditions for a fundamental change in the living environment and conditions of all Member States, but also determines the fact that a brand new *security*

[57] Stockholm Programme, 2009

concept and *security quality* is being shaped, both of the EU society itself and of each Member State.

This empirical study of security concept development in the context of globalisation has undergone a fundamental shift over the last decade. There has been a growing awareness among academicians that the public security actors are not the only organisation engaged in the process of maintaining global security.[58] This change in thinking is largely the result of the recent growth of the private security industry. In fact, in a globalization era, Member States faced with the importance of internal and external security are establishing an efficient common security 'network'. In many European countries, we could find a number of groups and officials other than public security institutions play key roles in the prevention of crime and the maintenance of public order. Indeed, governments have not discouraged the expansion of the regulatory roles currently being assumed by private security personnel, private investigators, special agencies and non-government policing organisations. For this reason, the traditional definition of "security" is required to be changed to a much wider understanding as concept of security.[59]

The publication also presents the outcomes of the research done by other researchers over the recent several years and dedicated to the diagnosis of the problems of globalisation and of national and international security in various regions of EU. The main attention

[58] Kalesnykas R. (2007). Privatization processes of policing in Lithuania. *SIAK Journal: Zeitschrift für Polizeiwissenschaft und Polizeiliche Praxis*. Wien: Bundesministerium für Inneres, No. 3, pp 14–24;

De Ward J. J. (1999). The private security industry in international perspective. *European Journal of Criminal Policy and Research*, Vol. 7(1), pp. 143–174

[59] Kalesnykas R. (2002). Possibilities to integrate the private security in the system of law and order. *Jurisprudence: Academic Journal of Mykolas Romeris University*, No. 26 (18), pp. 71–82

is focused on the analysis of threats and challenges in context of the EU integral security space.

The objective of the research is to evaluate new challenges, threats and prospects that could tantalize the security concept development and security trends of the EU Member States in the course of the globalisation processes. Therefore, in this paper will be briefly outlined the relationship between security and globalisation, security threats, risk and challenges to Member States and the new vision of the implementation of the EU Internal Security Strategy. Additionally, attention will be focused on the problems of security categorization. It is a topical issue, because in the security market the boundary between public and private interests in the area of safety and security needs becomes variable. The importance of the tasks mentioned earlier suggests that the theoretical and practical studies designed to better perceive and solve them can be considered as relevant both in a scientific and practical sense.

1. Globalization of security

In the context of globalisation, where any state's social and economic policy is frequently directed towards facilitating the movement of goods and services, finance and people, the economic opportunities created through such liberalisation can be associated with negative risks from corresponding easing of controls on criminal flows such as terrorism, counterfeit goods, drugs, illegal immigration, etc. Thus, increasing the need for security provision can be viewed as a negative outcome of global integration. Equally, increased economic and social integration can be seen to raise the level and extent to which security issues can spill over from one area to another, for example between different countries and regions, and with different levels of social and economic development.

Arguably, this raises the need for the greater adoption of common approaches and standards in security provision, for example in terms of greater EU-wide commonality in security policies and at a wider global level also.

1.1. Security risk society

Risk is described as the leitmotif of contemporary society. It is the combination of the likelihood of a future event and its possible impact. Risk has a dual nature. This means its perception may not necessarily be equal to its empirically measurable impact.[60] Duality presents a dilemma for managing risk, as the task is that of managing the risk itself as well as managing the fear of that risk. Risk society is the manner in which modern society organizes in response to security risks. According to A. Giddens, a risk society is "a society increasingly preoccupied with the future (and also with safety), which generates the notion of risk"[61], whilst the U. Beck defines it as "a systematic way of dealing with hazards and insecurities induced and introduced by modernisation itself".[62] Today, the welfare, progressive and democratic state, which was created in EU among Member States, is evolving into a risk society. In the context of risk society, the individual and/or organised citizen, the individual and/or organised business community, as well as the public authorities, focus all their political attention on crime, the subjective and/or objective feelings of insecurity and nuisance.[63] These traditional

[60] Slovic,P. (2000). *The Perception of Risk*. London: Sterling, VA: Earthscan Publications

[61] Giddens, A. (2003). *Runaway World: How Globalization is Reshaping Our Lives*. New York: Routledge

[62] Beck, U. (1992). *Risk Society, Towards a New Modernity*. London: Sage Publications

[63] The socio-economic added value of private security services in Europe (2013). Belgium: CoESS – Confederation of European Security Services

insecurities are supplemented by a fear of continuity related to, for example employment, social security, healthcare, food safety, financial security, the protection of privacy, migration, demography and the living environment.

Interpersonal perception patterns also change. In the risk society, what the people experience is more or less a 'moral panic'.[64] The new moral and global order must be based on a desire for security, safety and risk reduction. With the advent of the global economy, our society has acquired another dimension. As a result, it will be characterised by more and more economic free trade and finally proceed to a far advanced information society that is sustained by globalisation. In addition to the aforementioned globalisation, the debate among researchers on involving public or private responsibility for security and safety is under the microscope.[65] Private companies can therefore offer security services that seemingly belonged to the exclusive jurisdiction of the public authorities. One could argue that a growing dynamic between private sector security and public safety and law enforcement[66] has occurred. It is vital that private security entities work with public sector authorities seamlessly – at the state and federal levels – to share information and understand emerging risks and threats. The national and sovereign state is no longer the centre around which the political community is organised. The state remains an important player, which just like other players that compete with it, must prove its usefulness day after day. The individual citizen, who increasingly views the public authorities as a

[64] Beck, U. (1992). *Risk Society, Towards a New Modernity*. London: Sage Publications

[65] Kalesnykas, R. (2005). The threat as a dimension for security industry development. *Jurisprudence: academic journal of Mykolas Romeris University*, No. 76 (68), pp. 102–112

[66] Nemeth, Ch. P. (2017). *Private Security: An Introduction to Principles and Practice.* New York: Taylor & Francis

backdrop against which he or she must shape his or her life, wants above all to see measurable results when confronted with security and safety. In this respect, the market and market thinking has also made its entrance. Public authorities' performance must also be proportionate to fiscal efforts demanded from those very citizens. The business community is also put forward as a model. Actors from the private sector have succeeded, without any notable efforts, in capitalising on their understanding of the public sector. This will subsequently lead to increased and improved public authorities management.

These evolutions have led to a situation in which new, global, criminal phenomena are seen as risks and new security strategies become vital. Alongside and parallel with traditional public security actors, faced with old and new criminal phenomena, the ever-present private security sector has been able to develop further.[67] The aforementioned undercurrents have also brought about a situation in which private security management has become a sector with an international character and scope.

1.2. Multi-dimensional approach to the security concept

Security is of vital importance, but at the same time, it is not an independent concept. It is always related to individual or societal value systems.[68] Every actor talking about security assigns different meanings to the term.

[67] Pashley, V., Cools, M. (2012). Private Security in Europe: towards a European private security model for the future. In Cools, M., etc. *European criminal justice and policy*. Antwerpen: Maklu, pp. 93–114

[68] Brauch, H. G. (2005). *Threats, Challenges, Vulnerabilities and Risks in Environmental and Human security*. Bonn: United Nations University, Institute for Environment and Human Security

Based on the assumptions of the realist theory of international relations – that security is the dominant concern for states, that force is a major instrument, that governments preserve their unity as they interact with one another – security is achieved once threats to security can be prevented or at least managed. Contrary to the realist theory, social science theory perceives security as resulting from the interactions of various actors, with social values and identities shaping these relations. Security is accordingly intersubjective; constituted by a process of interaction and negotiation. Once the perception of security has changed, and the fear of one another is overcome, security is achieved.[69]

There have been various interpretations of security. In general, security has been understood to be synonymous with the accumulation of power. It has been regarded as a commodity, and power as the means of achieving it.[70] Within the organizational framework of the UN the focus has shifted away from a state-centred to a more human-centred approach. The concept of human security was included in the agendas of UN component organizations[71], and incorporated into the studies of the academic security community.[72]

[69] Brauch, H. G. (2011). Concepts of Security Threats, Challenges, Vulnerabilities and Risks. In Brauch, H.G., etc. *Coping with Global Environmental Change, Disasters and Security*. Berlin: Springer, pp 61–106

[70] Van Buuren, J. (2010). Security as a commodity. The ethical dilemmas of private security services. *INEX Policy Brief*, No. 6/2010. Oslo: International Peace Research Institute, pp. 1–5

[71] UN Department of Public Information (2004): A more secure world: our shared responsibility. Report of the High-level Panel on Threats, Challenges and Change. Retrieved from http://www.un.org/en/ga/search/view_doc.asp?symbol=A/59/565

[72] Brauch, H. G. (2005). *Threats, Challenges, Vulnerabilities and Risks in Environmental and Human security*. Bonn: United Nations University, Institute for Environment and Human Security

Despite a widening of the concept of security, a large number of states still adhere to a state-centred, militarized approach to the security.

Security is a basic requirement of every individual citizen. If it is not satisfied, it gives rise to insecurity, which can lead on to fear, discord and actual damage. Security moves the focus away from states and towards individuals. It emphasizes human rights, safety from violence, and sustainable development.[73] Seven dimensions of security are distinguished by the UN General Assembly:

1) economic security – assuring every individual a minimum requisite income;
2) food security – the guarantee of physical and economic access to basic foodstuffs;
3) health security – the guarantee of minimum protection from disease and unhealthy lifestyles;
4) environmental security – protecting people from the short- and long-term ravages of nature, man-made threats in nature, and deterioration of the natural environment;
5) personal security – protecting people from physical violence;
6) community security – protecting people from loss of traditional relationships and values and from sectarian and ethnic violence;
7) political security – ensuring that people live in a society that honours their basic human rights.[74]

Currently three different forms of conceptualizing security can be identified. The third way to conceptualize security is to understand

[73] Paris, R. (2001). Human Security: Paradigm Shift or Hot Air? *International Security*, Vol. 26, No. 2, pp. 87−102

[74] UN Department of Public Information. (2004). A more secure world: our shared responsibility. Report of the High-level Panel on Threats, Challenges and Change. Retrieved from http://www.un.org/en/ga/search/view_doc.asp?symbol=A/59/565

it as an encompassing concept, including all five dimensions of the widened concept of security: economic, societal, environmental, political, and military security.[75] Could be stated that ultimately, one concept – national security or human security – would gain a dominant position using security category in a global context.

1.3. Security categorization

Multidimensional nature of security results in both a society and industry that has no clear understanding of a definition for the concept of security. David J. Brooks in his studies poses a question "what are the knowledge categories and subordinate concepts of security?", responding to it that the most used security concepts in theory and practice are information security, followed by criminology and investigations and security management.[76] ASIS (American Society for Industrial Security) used common category named as integrated security systems. The ASIS practitioners/academics developed knowledge category descriptors of common security elements, consisting of: physical security, personnel security, information systems security, fire protection, risk management, legal aspects, emergency/contingency planning, loss prevention and investigations.

[75] UN Department of Public Information. (2004). A more secure world: our shared responsibility. Report of the High-level Panel on Threats, Challenges and Change. Retrieved from http://www.un.org/en/ga/search/view_doc.asp?symbol=A/59/565;

Brauch, H. G. (2011). Concepts of Security Threats, Challenges, Vulnerabilities and Risks. In Brauch, H.G., etc. *Coping with Global Environmental Change, Disasters and Security*. Berlin: Springer, pp. 61–106

[76] Brooks, D. J. (2010). What is security: definition through knowledge categorization. *Security Journal*, Vol. 23, Issue 3, pp. 225–239

In contrast, Hesse and Smith[77] proposed four knowledge categories appropriate for tertiary security education – security, business and management, computing and IT and generic. It was postulated that through academia, these knowledge categories would provide security managers with core knowledge for appointment in the security industry. Although these knowledge categories may be appropriate for generic supervisory or managerial occupations, the security knowledge categories did conflict to some degree with those proposed by ASIS International.[78]

David J. Brooks distinguishes the 13 security categories, but acknowledges that these categories require further academic and industry debate in order to gain a degree of consensus. These categories include the following security concepts:

1) security law (theories, principles, concepts, process and practices that consider how law affects organizational security);
2) security management (theories, principles, concepts, technique, process and practice of managing or controlling organizational resources to deliver the function of security. This category may include policy and procedures, administration, operations, training, awareness, resource allocation, security decay);

[77] Hesse, L., Smith, C. L. (2001). Core Curriculum in Security Science. In: H. Armstrong (ed.) *Proceedings of the 5th Australian Security Research Symposium*. Perth, Western Australia: School of Computing and Information Science, Edith Cowan University, pp. 87–104

[78] ASIS International (2010). *Proceedings of the 13th Annual Academic/ Practitioner Symposium*. Maryland: ASIS International, the University of Maryland. Retrieved from https://www.yumpu.com/en/document/view/5696591/proceedings-of-the-2009-academic-practitioner-asis-international

3) security technology (protection of assets using intruder detection systems, CCTV, access control, biometric systems);
4) physical security (theories, principles and concepts that use people in building environment to control access to an organization's assets);
5) industrial security (application aviation security, maritime security, critical infrastructure protection, government security, retail security, etc.);
6) security risk management (theories, principles, concepts and practices that considers risk and risk management. ISO 31000:2018 help organizations increase the likelihood of achieving objectives, improve the identification of opportunities and threats, effectively allocate and use resources for risk treatment);
7) safety (theories, principles, concepts and practices that consider a process for a safe and healthy work environment);
8) fire and life safety (theories, principles and concepts that consider treatment of fire and life safety, including building technology and the management of life safety and fire protection);
9) information and computing (theories, principles, concepts and practices that consider protection methods within the digital environment, including computer technology, hardware and software);
10) investigations (theories, principles, concepts and practices of security investigations, both process and technology);
11) facility management (the technique, process and practice of managing or controlling organizational resources to deliver the function of the built environment, in particular, an organization's facilities, for example facility design,

strategic planning, fixed plant and equipment, plant maintenance, energy management);

12) business continuity management (disaster, crisis, incident and business recovery that in general requires an initial response from government emergency services and support by site security, followed by further action from the organization itself;
13) criminology (theories, principles and concepts that consider the scientific study of crime and victimology, in particular, why crime is committed. This knowledge category may include principles such as crime prevention through environmental design).[79]

Categorization of security concept shows, that security at the strategic, managerial (tactical) or operational level cannot be considered singular in concept definition, as definition is dependent on context. Security context may be considered within the domains of international or national security, public security (policing), private or organizational security and individual security, to name a few.

2. European Union security and globalization

Understanding the awareness of security not only among EU citizens, but also among academics is changing it in the globalization phase. There exist different definitions of globalization. Clark defines globalization as an integration of economic, social and cultural relations across borders.[80] Today, many articles have gone beyond simple

[79] Brooks, D. J. (2010). What is security: definition through knowledge categorization. *Security Journal*, Vol. 23, Issue 3, pp. 225–239

[80] Clark, I. (1997). *Globalization and Fragmentation: International Relations in the 20th Century*. Oxford: Oxford University Press

restatement of basic arguments about economic globalization and discussion of political globalization and security globalization.[81] As Kay states, globalization is best understood as the creation of a variety of trans-boundary mechanisms for interaction that affect and reflect the acceleration of economic, political and security interdependence.[82]

Traditionally, national security is understood as pooling the efforts of the state and citizens to develop and consolidate democracy, to deter any potential attacker and defend the state's independence, territorial integrity and constitutional order. With re-conceptualization of security, there are using two dimensions:

1) *broadening,* i.e., consideration of non-military security threats, such as environmental scarcity and degradation, spread of disease, cross-border crimes, refugee movements, terrorism;
2) *deepening,* i.e., consideration of the security of individuals and groups rather than focusing narrowly on external threats to states, such as ethnic conflicts, civil war, environmental threats and survival of individuals. Yet, it is not easy to separate the agenda of discussions on broadening of security from globalization of security.[83]

[81] Hughes, C. W. (2002). Reflections on globalization, security and 9/11. *Cambridge Review of International Affairs*, No. 15(3), pp. 421–433

[82] Kay, S. (2004). Globalization, power and security. *Security Dialogue*, No. 35(1), pp. 10–11

[83] Karacasulu, N. (2006). Security and globalization in the context of international terrorism. *Review of International Law and Politics*, No. 2(5), pp. 1–17

2.1. Security risks and threats

The security threats facing the EU Member States are multifaceted, interrelated, complex and increasingly transnational in their impact and in that internal and external security are increasingly inseparable. No single Member State can achieve ‘high level’ or ‘better’ security alone. Nearly nine out of ten EU citizens believe that security questions should be dealt with not just at the national, but also at the EU level.[84] In this context, one of Europe’s main objectives is to preserve its values of open society and civil liberties while addressing the increased security threats.

Implementation of an efficient policy for EU security (internal and external) leads to development of a set of instruments covering law enforcement, intelligence, judicial, economic, financial and technological aspects. In a constantly changing and increasingly technological world, guaranteeing security without the support of knowledge and technology is almost impossible. Novel security solutions should provide ways to increase the security of our citizens without imposing additional unnecessary burdens on their daily lives. Technology makes it easier to detect dangerous materials being traded. The same applies to border controls, to prevent illegal immigrants, traffickers of human beings, drug traffickers and terrorists from taking advantage of the fact that internal border controls have been lifted within the Schengen area.[85] Innovative and

[84] Crime and criminal justice statistics (2015). Retrieved from http://ec.europa.eu/eurostat/statistics-explained/index.php/Crime_and_criminal_justice_statistics

[85] The Schengen Acquis – Convention implementing the Schengen Agreement of 14 June 1985 between the Governments of the States of the Benelux Economic Union, the Federal Republic of Germany and the French Republic on the gradual abolition of checks at their common borders, adopted by Council of The European Union decision No. 1999/435/EC of 20 May 1999. Retrieved from http://www.consilium.europa.eu/uedocs/cmsUpload/SCH.ACQUIS-EN.pdf

sophisticated solutions and systems will help avoid fraud on identity documents, inter alia through biometrics in visas, passports, residence permits and other documents.

Since all EU countries are facing common threats, should there be a shared 'European approach' for better security? The Internal Security Strategy (ISS) for the European Union: "Towards a European Security Model" sets out the widest possible mandate and lists nearly all conceivable threats and challenges for the EU: terrorism, serious and organized crime, cyber-crime, cross-border crime, violence itself, natural and man-mad disasters, as well as 'other common phenomena which cause concern and pose safety and security threats to people across Europe, for example road traffic accidents'.[86] These threats include typical security risks as:

1) terrorism: relating both to terrorist acts undertaken by (international) terrorist organisations and their affiliates, or by 'lone wolf' individuals. A broad definition of terrorism would cover both terrorism motivated by fundamentalist religious ideology and other forms of political and social ideological extremism;
2) criminality: primarily concerning illegal activity against property and persons for monetary gain. The main aspects of criminal activity that are of concern from a security policy perspective relate to "organised crime" engaged in "serious criminal activities" (e.g. drug trafficking, economic crime, human trafficking, smuggling of persons, arms

[86] Internal Security Strategy for the European Union: Towards a European Security Model, adopted by the Justice and Home Affairs Council on 25 February 2010 and endorsed by the European Council on 26 March 2010, No. 5842/2/10 REV 2 JAI 90. Retrieved from http://register.consilium.europa.eu/pdf/en/10/st05/st05842-re02.en10.pdf

trafficking, sexual exploitation of minors and child pornography, money-laundering and document fraud);

3) violations of public order and civil unrest: primarily concerned with widespread and mass violations of law and order (e.g. urban riots), that may be motivated by social or political causes. Threats associated to public order are addressed in a number of Member States' security policy and strategy documents;
4) espionage: which may concern economically motivated attempts to obtain information and data (e.g. industrial espionage) or be undertaken for political or ideological reasons;
5) migration (illegal): risks relating to illegal and irregular migration flows are identified in a number of Member States' security policy and strategy documents, even though they may be grouped alongside other 'cross border' concerns (e.g. cross-border movements of terrorists, organised criminals, and illicit goods).[87]

It also addresses the other challenges touched upon above, namely the need to better integrate internal and external aspects of security and the importance of respecting common fundamental norms, so as to arrive at a common 'European Security Model' for all involved actors. Nowadays, the most visible players in the EU security market are private security services. The private security sector also has an important role to play: developing appropriate

[87] Internal Security Strategy for the European Union: Towards a European Security Model, adopted by the Justice and Home Affairs Council on 25 February 2010 and endorsed by the European Council on 26 March 2010, No. 5842/2/10 REV 2 JAI 90. Retrieved from http://register.consilium.europa.eu/pdf/en/10/st05/st05842-re02.en10.pdf

security capabilities requires a strong and competitive industrial base, which itself depends on pinpointing the needs of customers for whom new products, systems and services are created. There are a number of cross-cutting policy issues that need to be addressed with a view to developing such a competitive industrial base and meeting the security needs of the public sector and of citizens. This includes improving the way systems operate together and inter-connect, mainly by developing common training standards[88], exchanging best practice and contributing to the reflection on improvement of procurement processes.

In many Member States it is believed that the trend for the public and private partnership of security forces is set to increase in the future with a view to strengthening preventive actions against threats and serious crimes, because private security is now an important force in many areas previously considered the responsibility of the state. This produces a ratchet effect. After yielding ground to the private sector, public authorities seem incapable of going backwards, often for financial reasons. Compatibility of activities of public and private security forces is linked with organisational-functional and legal presumptions. The author makes an assumption that a better EU security is to be expected out of compatibility of activities of the public and private security forces.

To summarise, we could claim that the Member States have their own national security policies and strategies. However, it has been considered that the Member States cannot respond to today's security challenges on their own, as most of these challenges are

[88] Kalesnykas, R. Dieninis, L. (2010). The legal regulation of professional requirements for private security personnel: the experience of Lithuania and some European Union countries. *Current Issues of Business and Law*, No. 5, pp. 223–241

cross-border. One could say that just a state can organise and implement an internal security strategy; however the EU is developing its own. On the other hand, we have agreed that in the EU, the security market was developing under different international, political, economic, social, legal and other conditions, which affected the nature, culture and qualities of different security forces, which plays the main role in implementing the EU Internal Security Strategy 2015–2020.

2.2. Security challenges

Today security has become so complex and multi-dimensional that the traditional national border-setting type of security perception is not capable of recognizing the new threats that transcend national borders. EU consists of more than 508 million people across the twenty-eight countries, which make up the EU. Economic growth, together with the opportunities provided by a free and democratic society based on the rule of law, generate prosperity among European citizens – but with such opportunities there also come risks, as terrorists, organized crime groups and other types of criminals seek to abuse those freedoms in the pursuit of destructive and malicious ends. Furthermore, in its turn the increased mobility of people increases our common responsibility for protecting the freedoms, which all citizens of the EU cherish.

As stated by Clark, a part of the broadening of the concept of security can be and has been attributed to the effects of globalization.[89] We have recognized that globalization challenges the EU Internal Security Strategy (2010), because with globalization

[89] Clark, I. (1997). *Globalization and Fragmentation: International Relations in the 20th Century*. Oxford: Oxford University Press

the divide between domestic (internal) and international (external) politics as well as the distinction between internal and external security is decreasing. Especial difficulties lies in the precise evaluation of the effects of globalization on EU internal security, because the impact of globalization varies from one EU region to another (Eastern to Western Europe) and is determined to a large extent by the state's capacity to meet the specific challenges presented by the process of globalization. Thus, it is not easy to generalize the stabilizing or destabilizing effects of globalization on EU internal security.

Firstly, globalization denotes that a nation (state) can no longer control non-physical security aspects, such as protection of information and technology assets. According to Kay[90], the more you protect your information and technology, the stronger you are. One of the challenges posed by globalization is that an individual Member State can no longer control the movement of technology and information. Europeanisation has blurred the division between the EU's internal and external security, so the Member States can no longer ignore the effects of globalization in forming their security policies.

Secondly, in the age of globalization, the emergence of information-based economies reduces the importance of national industries. For example, the increased foreign direct investment in local economies by multinational companies decreases a Member State's control of the domestic economy and makes it more vulnerable to international crisis and intervention, which is threatening its economic security.

[90] Kay, S. (2004). Globalization, power and security. *Security Dialogue*, No. 35(1), pp. 10–11

Thirdly, as the nature and strategy of EU internal security have changed, security threats have become more difficult to measure, monitor or tackle with the globalization process. There are non-state groups and individuals, such as ethnic groups, extremist groups, cults, organized crime and terrorism groups, which have been enhanced by the globalization of technology and information.[91]

Fourthly, globalization makes it easy for a Member State to reach to the weapons of mass destruction and other technologies, thus the Member State might pose the threats that are asymmetrical and disproportionate to their size. Today, a widely used term is the asymmetrical strategy (asymmetric power) following which a smaller power would attempt to defeat the largest powers in the globalized international system by striking against its perceived vulnerabilities.[92] Thus, globalization can give a chance to the strong Member States to enhance their powers; however, it also gives a chance for the weaker ones to challenge powerful ones.

Finally, summing up the challenges raised to EU internal security, it should be noted that globalization has a major impact on the implementation of the new EU internal security model. In the course of this process, the perception of security is changing, where the concept of security must be understood as a wide and comprehensive concept that straddles multiple sectors in order to address major threats and other challenges, which have a direct impact on the lives, safety, and well-being of EU citizens. Besides, every Member State should evaluate the threats and dangers posed to its national security within the framework of EU security.

[91] Cha, V. D. (2000). Globalization and the study of international security*. Journal of Peace Research*, No. 37(3), pp 391–403

[92] Ibid

3. Demand for new visions of security in the European Union

The EU aims to ensure that people live in an area of freedom, security and justice, without internal frontiers. Europeans need to feel confident that, wherever they move within Europe, their freedom and their security are well protected, in full compliance with the Union's values, including the rule of law and fundamental rights. In recent years new and complex threats have emerged highlighting the need for further synergies and closer cooperation at all levels. Many of today's security concerns originate from instability in the EU's immediate neighbourhood and changing forms of radicalisation, violence and terrorism. Threats are becoming more varied and more international, as well as increasingly cross-border and cross-sectorial in nature.

These threats require an effective and coordinated response at EU level. The European Agenda on Security[93] sets out how the EU can bring added value to support the Member States in ensuring security. Member States have the front line responsibility for security, but can no longer succeed fully on their own. While respecting national responsibilities for upholding the law and safeguarding internal security, all relevant EU and national actors need to work better together to tackle cross-border threats. The European Agenda on Security is a shared agenda between the EU and Member States. The result of its implementation is an EU area

[93] The European Agenda on Security, adopted the European Commission as Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on 28 April 2015, No. COM(2015) 185 final. Retrieved from https://ec.europa.eu/anti-trafficking/sites/antitrafficking/files/eu_agenda_on_security_en.pdf

of internal security where individuals are protected in full compliance with fundamental rights. To maximise the benefits of existing EU measures and deliver new and complementary actions, all security actors (EU public institutions and agencies, private companies & business associates, Member States and national security authorities) involved have to work together based on five key principles: maintaining full compliance with fundamental rights; transparent, accountable and democratic control giving citizens confidence; better application and implementation of existing EU legal instruments; joined-up inter-agency and a cross-sectorial approach and bringing together all internal and external dimensions of security.

3.1. Global Strategy for the European Union's Security Policy

In response to nowadays threats and risks which endanger people, organizations and Member States (terrorism, radicalism, hybrid threats, economic volatility, organized crimes, cyber-crime, illegal migration, etc.), in June 2016 the EU High Representative Federica Mogherini presented to the European Council a new Global Strategy for the EU's foreign and security policy: "Shared Vision, Common Action: A Stronger Europe".[94] This Global Strategy sets out EU core interests and principles for engaging in the Member States and other countries across world, and helps explain what the EU stands for and hopes to achieve.

[94] Shared Vision, Common Action: A Stronger Europe. Global Strategy for the European Union's foreign and security policy (2016), accepted in June 2016 by High Representative of the European Union for Foreign Affairs and Security Policy. Retrieved from http://eeas.europa.eu/archives/docs/top_stories/pdf/eugs_review_web.pdf

Global Strategy for the EU's foreign and security policy will pursue five priorities in its action:

1) Security of European Union. EU citizens should feel unprecedented security, democracy and prosperity. Member States must translate their commitments to mutual assistance and solidarity enshrined in the Treaties into action. The EU will step up its contribution to Europe’s collective security, working closely with its partners, beginning with NATO;
2) State and Societal Resilience. The EU invests in the resilience of states and societies to help them withstand and more quickly recover from conflict and crisis. Also, EU supports different paths to resilience, also via the EU enlargement policy and the European Neighbourhood Policy;
3) An Integrated Approach to Conflicts and Crises. EU will engage in a practical and principled way in peacebuilding, and foster human security through an integrated approach. Human security is at the core of all our actions and wherever EU acts at all stages of the conflict cycle, acting promptly on prevention, responding responsibly and decisively to crises, investing in stabilisation, and avoiding premature disengagement when a new crisis erupts. EU also stays engaged in the aftermath of conflict to ensure that peace is deeply rooted in society.
4) Cooperative Regional Orders. Regional governance makes it easier to manage security concerns, reap economic gains, and project influence. This is the rationale for the EU's own peace and development. EU works with regional organisations around the world;

5) Global Governance for the 21st Century. EU believes in the force of law rather than the law of force. EU is committed to a global order based on international law, which ensures human rights, sustainable development and lasting access to the global commons for everybody. A strong UN is the bedrock of the multilateral order, and the Sustainable Development Goals will drive reform in development policy.

In October 2016, Council of the EU adopted conclusions on the Global Strategy on the European Union's Foreign and Security Policy, in which it noted that the work on implementation of the EU global strategy should be focused on five priority areas:

1) resilience building and integrated approach to conflicts and crises;
2) security and defence;
3) strengthening the nexus between internal and external policies;
4) updating existing or preparing new regional and thematic strategies;
5) stepping up public diplomacy efforts.[95]

In addition, a strong focus on human rights, women, peace and security and gender equality and women's empowerment is a cross cutting priority for all EU Member States security policies.

It can be noted that Global Strategy on the European Union's Foreign and Security Policy is a “global” rather than an exclusively

[95] Council of the European Union conclusions on the Global Strategy on the European Union's Foreign and Security Policy, CFSP/PESC 813 CSDP/PSDC 571 (17 October 2016). Retrieved from http://data.consilium.europa.eu/doc/document/ST-13202-2016-INIT/en/pdf

“security” strategy. Above all it provides a coherent perspective for the EU’s internal and external action as a whole, as warranted by the Treaty on European Union. Security is an essential component for each EU Member State, but the full strength and value of such concept are fulfilled only when it is deployed alongside other external policies – such as enlargement, development and trade – or policies with external aspects, including on migration, energy, climate, environment, culture and more. This unique mix of actions is the European way to common security policy. The European Council and the Commission concurred that such a “whole of the EU” approach should be pursued in the implementation phase of the Global Strategy on the European Union's Foreign and Security Policy as well, and has been reflected in the EU’s regional and geographical priorities.

3.2. European Union internal security strategy

The growing process of Europeanization, especially in its top-down form, has influenced the internal security issues of the Member States, in particular those forming the external borders of the EU. The European Council is convinced that the enhancement of action at the EU level, combined with a better coordination with actions at the regional and national levels, is essential to protection against trans-national threats. The main crime-related risks and threats facing Europe today continue to challenge EU security. Wide – spread cross-border crime has become an urgent challenge, which requires a clear and comprehensive response. Whilst in itself not aimed at creating any new competences, but at integrating existing strategies and conceptual approaches, and acknowledging the framework of the Stockholm Programme[96], the Council of the European Union has adopted the Internal Security Strategy for the European Union: "Towards a European Security Model" 2010–2014[97] (hereinafter – Internal Security Strategy), which is a response to this situation.

The main aim of the Internal Security Strategy is to harness and develop common tools and policies to tackle common threats and risks using a more integrated approach. To achieve that aim, Internal Security Strategy defines 10 strategic guidelines. Each Member State must provide the following guidelines for action:

1) a wide and comprehensive approach to EU security;
2) democratic and judicial supervision of security activities;
3) prevention and anticipation: a proactive, intelligence-led approach;
4) developing a comprehensive policy of information sharing;
5) operational cooperation;
6) synergies with judicial cooperation in criminal matters;
7) integrated border control and management;
8) innovation and training;
9) strengthening the external dimension (cooperation with third countries);
10) flexibility and adaptation to emerging future challenges.

[96] The Stockholm Programme – an open and secure Europe serving and protecting citizens, approved by Council of the European Union on 2 December 2009, No. 16484/1/09 REV 1 JAI 866 + ADD. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=LEGISSUM%3Ajl0034

[97] Internal Security Strategy for the European Union: Towards a European Security Model, adopted by the Justice and Home Affairs Council on 25 February 2010 and endorsed by the European Council on 26 March 2010, No. 5842/2/10 REV 2 JAI 90. Retrieved from http://register.consilium.europa.eu/pdf/en/10/st05/st05842-re02.en10.pdf

These strategic objectives set out in the Internal Security Strategy 2010–2014 remain valid and should continue to be pursued. Council of the European Union has renewed and adopted a new Internal Security Strategy 2015–2020, in which are set up five strategic objectives for the EU and its Member States to pursue in order to increase effectiveness in combatting and preventing serious and organized crime, terrorism and cybercrime, to enhance the management of our external borders and to foster resilience to natural and man-made disasters.

It demonstrates an EU commitment to continuing making progress in the Area of Justice, Freedom and Security through Internal Security Strategy. On the other hand, it faces the following challenges: protecting rights and freedoms; improving cooperation and solidarity between Member States; addressing the causes of insecurity and not just the effects; prioritising prevention and anticipation; involving all sectors with a role to play in public protection (political, economic, social, etc.); communicating security policies to the citizens; and, finally, recognising the interdependence between internal and external security in establishing a “global security” approach with third countries.

Many of today’s security challenges are cross-border and cross-sectoral in nature. No single Member State is able to respond to these threats on its own. This is something that worries our citizens and businesses. Four out of five Europeans want more action at the EU level against organised crime and terrorism.[98] Much has been achieved to respond to those emerging threats and to

[98] Special Eurobarometer 464b. Report “Europeans’ attitudes towards security” (2017). European Union

increase Europe's security. With the Lisbon Treaty[99] in force, and with the guidance provided by the Stockholm Programme[100] and its Action Plan, the EU now has the opportunity to take further determined action. Internal Security Strategy 2015–2020 set out the challenges, principles and guidelines for dealing with these issues within the EU and called on the Commission to propose actions for implementing this strategy. The Communication of the European Commission "European Agenda on Security"[101] builds on what the Member States and EU institutions have already agreed, and proposes how Member States can work together over the next five years to be more effective in:

1) tackling terrorism and preventing radicalisation;
2) disrupting serious and organised crime, especially cross-border crime;
3) fighting cybercrime.

We could infer that the measures settled in the Internal Security Strategy 2015–2020 will help to resolve the main challenges for the security of the EU. Crime takes advantage of the

[99] Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community, signed at Lisbon, 13 December 2007. *Official Journal*, 2007/C 306/01. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:12007L/TXT

[100] The Stockholm Programme – an open and secure Europe serving and protecting citizens, approved by Council of the European Union on 2 December 2009, No. 16484/1/09 REV 1 JAI 866 + ADD. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=LEGISSUM%3Ajl0034

[101] The European Agenda on Security, adopted the European Commission as Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on 28 April 2015, No. COM(2015) 185 final. Retrieved from https://ec.europa.eu/anti-trafficking/sites/antitrafficking/files/eu_agenda_on_security_en.pdf

opportunities offered by a globalised society, such as high-speed communications, high mobility and instant financial transactions. A number of significant common threats can be managed by commitment of all actors concerned to do more and to work better together. This includes EU institutions, Member States and EU agencies. It requires a global perspective with security as one of our main external priorities. The EU must be able to react to unexpected events, seize new opportunities, anticipate and adapt to future trends and security risks.

To sum up, it can be assumed that the EU must consolidate the Internal Security Strategy based on the principles and values of the EU, namely, respect for human rights and fundamental freedoms, the rule of law, democracy, dialogue, tolerance, transparency and solidarity. The quality of our democracy and public confidence in the EU will depend to a large extent on our ability to guarantee security and stability in Europe and to work with our neighbours and partners to address the deeply rooted causes of the security problems faced by the EU.

Conclusions

1. Highlighting the multidimensional nature, the concept of security is difficult to define. However, the research study proposed that the concept of security may be defined when understanding it in an applied context. By developing and presenting a deep consensus of knowledge within the applied context, concept definition may be used in a global context. Security may be considered as assured freedom from poverty or want, precautions taken to ensure against theft, espionage or a person or a thing that secures or guarantees.

2. The demand and need for a new-style of security services, the development of security market and creation of the common security standards for Member States promoted by the processes of globalisation within the changing global society. This leads mixed challenges in each Member State as regards to management of new risks and combating of new threats: terrorism, serious and organised crime, drug trafficking, cybercrime, trafficking in human beings, sexual exploitation of minors and child pornography, economic crime and corruption, smuggling of persons and trafficking in arms, etc. Furthermore, the rapid penetration of the globalisation process into the security market poses new risks and threats to safety of the EU's citizens and the EU's security policy too.
3. The author observes that some challenges in certain EU countries may be regarded as a threat to security: mass growth, organised crime, terrorism, radicalisation and recruitment, cybercrime, privatisation of security services. The author raises the question: how the European Security Model should look like to make the situation in the EU security field not as bad as it is now, moreover, what should be done to improve it? In solving the problem, the author explains how the renewed EU Internal Security Strategy 2015–2020 is capable of implementing security and safety needs for citizens and maintaining the high-level of security space in every Member State.
4. The author claims that security services in a globalised world may exist as a business, whereas the efficiency of the security services depends on competition among various security service providers. Thus, it could be maintained that tendencies of the privatisation of security services are a new social phenomenon, which influences the EU's security policy and gives rise to

academic and practical debates. The issue of the privatisation of security services is treated as the process of transference of certain obligations of EU security enforcement and responsibilities from public security services to private security services.

5. The Treaty of Lisbon, the Stockholm Programme, European Agenda on Security, the Global Strategy on the European Union's Foreign and Security Policy have identified the fundamental principles and guidelines for actions in the development of the EU Internal Security Strategy 2015–2020. Every Member State must prepare its homework well in order to implement the EU Internal Security Strategy and at the same time strengthen the area of freedom, security and justice. We should not forget that every new strategy challenges relevant changes. In order to avoid this, it is necessary to establish the standards and criteria of evaluation of the effectiveness of the Internal Security Strategy, for each Member State to prepare national programs on national/ public security and safety and to allocate an appropriate amount of funds to implementation of the measures stipulated in such programmes.
6. EU Internal Security Strategy 2015–2020 has contributed to the reinforcement of the capacities of the EU and of its Member States with regard to operational cooperation, and to a cross-cutting approach, by linking its external dimension to the Internal Security Strategy. New challenges and a set of emerging threats in the European framework will necessarily mean greater vertical and horizontal cooperation between countries and between security forces, security actors and security services providers.

References

ASIS International (2010). Proceedings of the 13th Annual Academic/Practitioner Symposium. Maryland: ASIS International, the University of Maryland. Retrieved from https://www.yumpu.com/en/document/view/5696591/proceedings-of-the-2009-academic-practitioner-asis-international

Beck, U. (1992). *Risk Society, Towards a New Modernity*. London: Sage Publications

Brauch, H. G. (2005). Threats, Challenges, Vulnerabilities and Risks in Environmental and Human security. Bonn: United Nations University, Institute for Environment and Human Security

Brauch, H. G. (2011). Concepts of Security Threats, Challenges, Vulnerabilities and Risks. In Brauch, H.G., etc. *Coping with Global Environmental Change, Disasters and Security*. Berlin: Springer, pp. 61–106

Brooks, D. J. (2010). What is security: definition through knowledge categorization. *Security Journal*, Vol. 23, Issue 3, pp. 225–239

Cha, V. D. (2000). Globalization and the study of international security. *Journal of Peace Research*, No. 37(3), pp. 391–403

Clark, I. (1997*). Globalization and Fragmentation: International Relations in the 20th Century*. Oxford: Oxford University Press

Crime and criminal justice statistics (2015). Retrieved from http://ec.europa.eu/eurostat/statistics-explained/index.php/Crime_and_criminal_justice_statistics

De Ward, J. J. (1999). The private security industry in international perspective. *European Journal of Criminal Policy and Research*, Vol. 7(1), pp. 143–174

Giddens, A. (2003). *Runaway World: How Globalization is Reshaping Our Lives*. New York: Routledge

Held, D., McGrew, A., Goldblatt, D., Perraton, J. (1999). *Global Transformations: Politics, Economics and Culture*. Stanford, Stanford University Press

Hesse, L., Smith, C. L. (2001). Core Curriculum in Security Science. In: H. Armstrong (ed.) Proceedings of the 5th Australian Security Research Symposium. Perth, Western Australia: *School of Computing and Information Science*, Edith Cowan University, pp. 87–104

Hughes, C. W. (2002). Reflections on globalization, security and 9/11. *Cambridge Review of International Affairs*, No. 15(3), pp 421–433

Kalesnykas, R. (2002). Possibilities to integrate the private security in the system of law and order. *Jurisprudence: Academic Journal of Mykolas Romeris University*, No. 26 (18), pp 71–82

Kalesnykas, R. (2005). The threat as a dimension for security industry development. *Jurisprudence: academic journal of Mykolas Romeris University*, No. 76 (68), pp. 102–112

Kalesnykas, R. (2007). Privatization processes of policing in Lithuania. *SIAK Journal: Zeitschrift für Polizeiwissenschaft und Polizeiliche Praxis*. Wien: Bundesministerium für Inneres, No. 3, pp. 14–24

Kalesnykas, R. Dieninis, L. (2010). The legal regulation of professional requirements for private security personnel: the experience of Lithuania and some European Union countries. *Current Issues of Business and Law*, No. 5, pp. 223–241

Karacasulu, N. (2006). Security and globalization in the context of international terrorism. *Review of International Law and Politics*, No. 2(5), pp. 1–17

Kay, S. (2004). Globalization, power and security. *Security Dialogue*, No. 35(1), pp. 10–11

Nemeth, Ch.P. (2017). *Private Security: An Introduction to Principles and Practice*. New York: Taylor & Francis

Paris, R. (2001). Human Security: Paradigm Shift or Hot Air? *International Security*, Vol. 26, No. 2, pp. 87−102

Pashley, V., Cools, M. (2012). Private Security in Europe: towards a European private security model for the future. In Cools, M., etc. *European criminal justice and policy*. Antwerpen: Maklu, pp. 93–114

Slovic, P. (2000). *The Perception of Risk*. London; Sterling, VA: Earthscan Publications

Special Eurobarometer 464b. Report "Europeans' attitudes towards security" (2017) European Union

The socio-economic added value of private security services in Europe (2013). Belgium: CoESS –Confederation of European Security Services

UN Department of Public Information (2004): A more secure world: our shared responsibility. Report of the High-level Panel on Threats, Challenges and Change. Retrieved from http://www.un.org/en/ga/search/view_doc.asp?symbol=A/59/565

Van Buuren, J. (2010). Security as a commodity. The ethical dilemmas of private security services. *INEX Policy Brief*, No. 6/2010. Oslo: International Peace Research Institute, pp. 1–5

Council of the European Union conclusions on the Global Strategy on the European Union's Foreign and Security Policy, CFSP/PESC 813 CSDP/PSDC 571 (17 October 2016). Retrieved from http://data.consilium.europa.eu/doc/document/ST-13202-2016-INIT/en/pdf

Internal Security Strategy for the European Union: Towards a European Security Model, adopted by the Justice and Home Affairs Council on 25 February 2010 and endorsed by the European Council on 26 March 2010, No. 5842/2/10 REV 2 JAI 90.

Retrieved from http://register.consilium.europa.eu/pdf/en/10/st05/st05842-re02.en10.pdf

Renewed European Union Internal Security Strategy 2015–2020, approved by the European Council on 10 June 2015, No. 9798/15. Retrieved from http://data.consilium.europa.eu/doc/document/ST-9798-2015-INIT/en/pdf

Shared Vision, Common Action: A Stronger Europe. Global Strategy for the European Union's foreign and security policy (2016), accepted in June 2016 by High Representative of the European Union for Foreign Affairs and Security Policy. Retrieved from http://eeas.europa.eu/archives/docs/top_stories/pdf/eugs_review_web.pdf

The European Agenda on Security, adopted the European Commission as Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on 28 April 2015, No. COM(2015) 185 final. Retrieved from https://ec.europa.eu/anti-trafficking/sites/antitrafficking/files/eu_agenda_on_security_en.pdf

The Schengen Acquis – Convention implementing the Schengen Agreement of 14 June 1985 between the Governments of the States of the Benelux Economic Union, the Federal Republic of Germany and the French Republic on the gradual abolition of checks at their common borders, adopted by Council of The European Union decision No. 1999/435/EC of 20 May 1999. Retrieved from http://www.consilium.europa.eu/uedocs/cmsUpload/SCH.ACQUIS-EN.pdf

The Stockholm Programme – an open and secure Europe serving and protecting citizens, approved by Council of the European Union on 2 December 2009, No. 16484/1/09 REV 1 JAI 866 + ADD. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=LEGISSUM%3Ajl0034

Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community, signed at Lisbon, 13 December 2007. *Official Journal*, 2007/C 306/01. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:12007L/TXT

About the Author

Raimundas Kalesnykas, *Prof. Dr.*
Raimundas Kalesnykas is lecturer at the Faculty of Law of the Kazimieras Simonavicius University in Vilnius, Lithuania. He graduated in law and security studies within security manager specialization (BA, Master and PhD) at the Law University of Lithuania. Raimundas Kalesnykas has more than 20 years of professional experience as researcher, academic, trainer (ToT), published more than 50 books and research papers, presented research results over 80

international scientific conferences in Lithuania and abroad, as a invited professor visited over 60 foreign universities for lecturing, successfully implemented over 30 international projects on issues of security and anti-corruption risk management and strategical solutions, police, criminal justice and security sector reform. He has over 14 years' professional experience working as a key security and anti-corruption expert in OSCE, USAID, Saferworld and other international organizations. Today, he acting as a Director of the National Anti-Corruption Association (NACA) in Lithuania and certified consultant and auditor of anti-corruption standards (ISO 37001, ISO 19600).

Part II

Security management

GUARDING SERVICES

Kaci Bourdache

Introduction

This article aims to highlight the most important and noteworthy issues in guarding services and how they can be used effectively. After reading, you should have an understanding of the scope of guarding services available and how they can be used as part of Safety & Security Risk Management. Hopefully, this will allow you to plan accordingly and use guarding services to their full effect and integrate the use of that service to the management of a wide variety of safety and security risks in an organization.

Private Security Services have grown in the past decades. Researchers in the field have proposed quite a few of explanatory factors, according to the research of van Steden, they are as follows:

1) rising crime and related problems;
2) growth of mass private property;
3) economic rationalities;
4) government policy toward private sector participation;
5) overburdened police force;
6) professionalization of private security.

Considering these factors, it is no wonder that private security – which includes guarding services – has increasing importance.[102] In the future there may be a blending of law enforcement with security officer in some assignment, a mixture of a kind.[103]

[102] van Steden, R. (2007). *Privatizing Policing, Describing and explaining the growth of private security*. BJU Legal Publishers

[103] Zalud, B. (2010). *Tech-Armed Officers on Future's Watch, Security in 2020*. ASIS International

1. Guarding services as a risk management measure

1.1. Role of Guarding Services in Safety & Security Risk Management

According to the standard ISO 31000:2018 Risk Management guidelines, *risk management* refers to coordinated activities to direct and control an organization with regard to risk, ie. the effect of uncertainty on objectives. Controlling a risk refers to measures that maintain and/or modifies risk, such as a process, policy, device, practice, or other condition and/or action which maintain and/or modify risk.[104]

The variety of risks that the risk management standard covers are very varied, but in the context of this article we will discuss specifically *safety* and *security* risks, as well as their control with guarding services. A crude but simple way to define safety and security would be to understand safety as a condition where one is adequately protected against threats of accidental nature, and security when those threats are human; negligence, carelessness or malicious intent all included. Managing safety and security risks in an organization is often simpler if they are conceptualized into different elements, such as information security, occupational safety, cybersecurity, emergency preparedness, physical security and environmental safety. The elements often intersect in practice, but managing risks in each domain with the proper resources is vital.

Risk treatment refers to selection and implementation of ways for addressing risks. That is further divided into categories which are listed below, with emphasis added on categories in which guarding services have direct value in the context of safety and security.

[104] ISO 31000:2018 Risk management. Guidelines. Rerieved from https://www.iso.org/iso-31000-risk-management.html

Table 1

Risk treatment categories[105]

Avoiding the risk by deciding not to start or continue with the activity that gives rise to the risk
Taking or increasing the risk in order to pursue an opportunity
Removing the risk source
Changing the likelihood
Changing the consequences
Sharing the risk (e.g. through contracts, buying insurance)
Retaining the risk by informed decision

In the following subchapters, the specific ways in which guarding services can be used as a risk treatment method are explored further.

Deterrence, Prevention and Preparedness

In the context of risk management, these would all apply to changing the *likelihood* of risks. *Deterrence* means prevention specifically by deterring a person, ie. by influencing their decision-making. In plain terms, the potential perpetrator of a crime or other frowned activities will refrain from action, because they feel that it is too risky for them. With guarding services, such a deterring effect can be achieved by uniformed guards visible to the public; they send a message that the site is guarded and immediate response is available.[106] It is crucial that the guards project alertness and the capacity for action; but also a certain approachability, as security guards tend to invite general questions from customers and such.

[105] ISO 31000:2018 Risk management. Guidelines. Retrieved from https://www.iso.org/iso-31000-risk-management.html

[106] Ricks, T. & Ricks, B. & Dingle J. (2015). *Physical Security and Safety, a Field Guide for the Practicioner*. Boca Raton: CRC Press

Proper customer service – such as greeting people or otherwise establishing that they have been noticed – is not only good manners, but also a very effective deterrent. Planning effective use of the guards' locations, rounds and timetables for maximum effect is important. In case of guarding rounds to enhance visibility, the rounds are preferably regularly irregular, ie. happen at certain time windows but never at exactly the same times or intervals. In absence of guard presence, indicating the existence of security guards with plaques and signs is also a good idea.

In addition to only deterrence, there is a multitude of ways that guards can perform *prevention* for a variety of safety & security risks. Prevention as a whole applies to all possible measures that lower likelihood of risks realising. This can be achieved by removing or influencing the causes that lead to the undesired effects. Examples include removing fire and accident hazards, locking doors, notifying of structural or technical defects, etc. This can be achieved by regular rounds, assisted by surveillance systems.

Preparedness refers to all arrangements that are in place in anticipation of a threat realizing. Often they are mandated by law, especially in occupational safety and fire safety. Examples are first aid arrangements from equipment to first aid training, fire extinguishers and fire compartmentalization as well as all fire safety training. Preparedness in security refers to the upkeep and readiness of detection and response, like having a sufficient guard presence and surveillance system in place. Security guards can assist in the upkeep of preparedness to make sure that all of the arrangements are properly in place, maintained, accessible and in working order. They can identify and record concerns such as broken windows or locks, loose steps, lights out or emergency exits blocked.[107] Most

[107] Ricks, T. & Ricks, B. & Dingle J. (2015). *Physical Security and Safety, a Field Guide for the Practicioner*. Boca Raton: CRC Press

importantly, guards should make sure that they themselves can upkeep proper physical and mental readiness as well as correct equipment for a variety of situations.

Surveillance and Detection

Surveillance and detection refers to constant monitoring via technical surveillance means as well the natural senses of a person. It is important to note that though artificial intelligence and automation is developing constantly, it is still almost impossible to provide a full surveillance system that is able to escalate towards a proper response without a human element somewhere in the chain. The natural senses combined with cognitive abilities of a security guard for example cannot currently be fully replaced with technology. Planning adequate surveillance is important, and it overlaps with prevention. The key issue here is to have a sufficient, cost-effective coverage that allows the detection of the risks that occur despite the preventive measures done. According to Ricks et al., applying one person to multiple jobs decreases the efficiency of that person, so sufficient focus in duties is recommended. The weakness of relying on guards only in surveillance and detection is coverage; they simply cannot see or hear that far. Planned, regular surveillance rounds help, but usually sufficient detection requires two things: cooperation with the staff and use of technology to assist.[108]

Making sure that the whole staff is able and willing to keep their eyes open and to report to the security personnel multiplies the coverage of surveillance considerably. This requires proper training, guidelines and motivation for the whole staff, as well as meshing security guards closely to the staff of any facility that they

[108] Ricks, T. & Ricks, B. & Dingle J. (2015). *Physical Security and Safety, a Field Guide for the Practicioner*. Boca Raton: CRC Press

guard. In other words, guards should not be the only ones who are given responsibility, and they should not be treated as a completely separate entity from the entire staff. Smart use of technology – e.g. performing regular camera rounds and instant notifications from e.g. ventilation, fire or intruder detection systems facilitate the work that guarding services do and allows them to maintain surveillance without physical presence.

Response and Counter–measures

Response is the planned reaction when a threat is detected. From the perspective of guarding services, it typically refers to immediately informing one or more security guards and dispatching them to the exact location of alarms, fires or other safety or safety concerns; determining a proper response requires a detailed analysis based on the threats.[109] The planned response is described in the guarding contract. In addition to the contract however, the security guards themselves should always be able to assess the situation and request additional response when necessary; preferably anticipatory response, before the threat cannot be contained. The additional response can include other security guards as well as the authorities and other public safety operators, such as fire and rescue, emergency medical services and the police. Obviously these are not included in the guarding contracts, but they are still part of the response chain and should be included in the planning.

The main task of security guards responding to a threat is to initiate proper *counter-measures.* First, it is vital to assess the situation, then evaluate the need for further response (assistance), and to do the necessary procedures to protect life, health, and

[109] Ricks, T. & Ricks, B. & Dingle J. (2015). *Physical Security and Safety, a Field Guide for the Practicioner*. Boca Raton: CRC Press

property – roughly in that priority order. The ability of a security guard to function is through training and equipment higher than the average person, but not as high as professional first responders. Compare e.g. to a police patrol responding to a threatening or violent person, or firemen responding to a fire or accident. Like any person, a guard should not take unnecessary risks and mind their own health and well-being. That being said, they should do their utmost to protect the assets that they are assigned to guard. Specific countermeasures vary based on the threat and the situation. A few examples.

Table 2

Security guard countermeasure examples

Situation	Countermeasures
Accident or injury	Prioritization, administer emergency first aid, support first responders, prevent further accidents
Fire	Extinguishing, limiting fire (doors, windows, ventilation), setting in motion or assisting in evacuation, supporting first responders, protecting premises from further damage
Crime scene	Preventing further damage, protecting scene from contamination, guarding exposed premises and property, assisting police
Criminal act	Preventing further injury or damage, protecting victim, if possible apprehending suspect, assisting police
Threatening person or violent attack	De-escalation, stopping the attack, use of force if necessary, if possible apprehending suspect, assisting police
Water damages	Stopping water at source, dam up the flow, protecting loose property

Finally, it is important to note that after all situations security guards should report their observations and actions in writing after the situation has been resolved. This will protect the legal and contractual obligations of all parties, and allow for further development of safety and security.

1.2. Should you use guarding services?

Using guarding services is not always simply an additional operation; one way or another, you are outsourcing some activities. That is in the end a financial decision, one that should not be done lightly. However, there are clear benefits in outsourcing. According to Johnson & Ortmeier and Halibozek & Kovacich these could be.

Table 3

Benefits of outsourcing security personnel[110]

Lower cost	Outsourced employees generally cost less, and have less hidden costs (fair warning however: if you pay cheap, you get cheap)
Administrative unburdening	The contractor is responsible for hiring, training, equipping, scheduling, supervising, evaluating and terminating employees
Flexibility	As security needs change, the number of contract personnel required can be increased or decreased easily
Fewer direct personnel issues	Security personnel are managed indirectly, as client simply supervises obligations of contract, while the management of the outsourced company handles daily personnel issues.
Objectivity	Contract employees are likely to be more objective and less susceptible to collusion with nonsecurity employees of the host company or agency
Expertise	In some cases, organizations have specific and specialized security needs that they cannot meet. A specialized contract agency can provide these services. According to Zalud (2010), training for security officers in the future will be longer, deeper and more complex than it is now.[111]

[110] Johnson, B. & Ortmeier, P. (2018). *Introduction to Security, Operations and Management*. Pearson Education;

Halibozek, E. & Kovacich, G. (2017). *The Manager's Handbook for Corporate Security*. Elsevier Inc.

[111] Zalud, B. (2010). *Tech-Armed Officers on Future's Watch, Security in 2020*. ASIS International

In addition to the above, local legislation should be considered. In some countries, only contracted security guards are considered true security guards, and only they have the full rights and responsibilities by law. Considering all of this, if guarding services seem like a good solution, chapter 2 will discuss the variety of services in detail.

2. Variety of guarding services

In the following subchapters, different guarding services will be discussed, mostly in the context of physical security. National legislation as well as e.g. insurance company guidelines may impose requirements on varying services, but by and large the services below have evolved naturally, as guarding service companies vie to fulfil the needs of customers. In other words, legislation usually has a few general strokes or some minor details that need to be taken into account for some guarding services more than others, but for the most part all guarding services and security guards are legally the same thing. The effects of legislation as a whole to the industry are covered with more detail in chapter 2. Here, we will focus on the service aspects.

2.1. Static guarding

Static guarding refers to a security guard or guards who do not leave the premises they are assigned to during their work shift. The actual duties in static guarding can vary greatly, emphasising different needs and skillsets of the client. In general, static guarding has both *continuous tasks* and *timed tasks*. The former refers to tasks that the guard does continuously from their assigned location or locations; they are usually more general in nature and include for example access control, surveillance of security systems, customer service and overall security surveillance at that location. Timed tasks refer to tasks that must be completed at certain times (e.g. 8:00 sharp) or certain time windows (e.g. between 7.00 and 9.00). Typical timed tasks are for example surveillance rounds, closing or opening rounds, certain customer service situations such as receiving deliveries or providing special protection for certain events such as visits or meetings.

In addition to these general tasks, static guarding also includes the concept of *control room guarding*, where the surveillance of security systems and their outputs on monitors and reports, with related customer service, is the most critical task. The guard in a control room is typically in charge of situation control and informing other guards in the field, as well as is the primary person for reporting and any outside communication towards e.g. the client representative, maintenance or authorities. As far as skillsets go, they require good command of surveillance systems and IT equipment. Some of the control room tasks may also be completed in *reception*, but as a whole these duties emphasize access control and customer service. Maintaining a good, up-to-date situation picture of any visitors or other people on site is crucial, while making sure that no unauthorized access occurs. A firm but friendly demeanour is required, as well as customer service and language skills.

2.2. Mobile guarding

Mobile guarding, as opposed to static guarding, refers to guards that move from one contracted client's task towards another contracted client constantly during their work shift. The tasks are typically timed, as in static guarding, either with exact times or certain time windows during which the task must be performed.

Therefore, mobile guards follow a certain time sheet of tasks, located in different locations. Apart from the time needed to move between these locations, downtime should be minimised. This is of course not the concern of the client, who only pays for the certain procedure that needs to be done; which can take anywhere between a few minutes to hours. Static guarding is a lot more expensive, as the client is paying for a constant service. If that is not needed and timed tasks provide adequate security for their needs a mobile guarding contract is more efficient.

From the perspective of the guards performing this service, a good sense of scheduling and personal responsibility is needed; not to mention stress tolerance and the capacity to deal with rapid changes. Most often mobile guards use vehicles to move between locations, but other methods of transportation like bicycles or moving on foot are just as valid; it all depends on time, distance and cost-effectiveness. This being said, extra care on rest periods and traffic safety is paramount. A final important point pertaining to scheduling in this service type is *alarm guarding* – this refers to a service that mobile guards often provide as part of their daily routines, where they receive notifications of alarm system detections via an alarm centre operator (see 2.4.), move to the location, determine cause of alarm and initiate necessary countermeasures.

2.3. Loss prevention

Loss prevention, in the context of guarding services, refers to security guards that specialize in supply chain loss prevention, specifically via criminal loss such as theft and embezzlement. Retail loss prevention is the most common duty, in which security guards, often called *store detectives,* attempt to uncover crimes by the clients and, occasionally, of staff as well by constant surveillance. In these tasks the guards wear regular clothing as opposed to uniforms, so that they can blend in with the clientele. With possible support from control room guards with access to camera surveillance, they can follow persons under suspicion and attempt to detect any thefts or theft attempts as they occur. After this, they can stop the crime from happening and/or detain the suspects (depending on national legislation); however, it is beneficial to have uniformed guards to perform the apprehending, if possible. In that way the store detectives can remain unidentifiable to the perpetrator.

In the retail market, *mystery shopping* services are at times used to ascertain the level and competence of customer service. Security service providers also provide this at times, but with an eye towards criminal acts, such as embezzlement, perpetrated by the staff. These services are often called upon when such criminal activity among staff is already suspected to occur. In staff-related crimes, direct theft can also be prevented in the supply chain by performing exit checks; during these staff are subject to searches when leaving the premises. It is good to note however that usually employees have legal right to refuse, so great care and tact must be observed in this and all loss prevention positions.

2.4. Alarm centre and Remote surveillance

Alarm centre services provide the crucial link between surveillance technology and any reaction or countermeasures. Alarm centre dispatchers receive notifications if any system contracted and connected to their centre relays an alarm, after which they act upon it as agreed in the client contract, based on the type of alarm which can vary from intruder detection to fire or water leak sensors. Typically this means alerting the contact person to make sure that the alarm was not accidental; the alarm can be cancelled with a proper password. Correct action can also mean tapping into remote surveillance cameras. Finally, the alarm centre can alert a guard to the location, or even the appropriate authorities if e.g. camera surveillance confirms the alarm as an actual, immediate threat such as a fire or a robbery. Surveillance systems can of course always alert the owner of the system or premises, but if they are unable to act upon the alarm information, it is close to useless. With proper alarm centre plus alarm guarding services, the client can have a greater piece of mind that even in their absence situations are investigated and countermeasures activated.

Remote surveillance is very close to alarm centre services and indeed these are often done concurrently. The main difference is that instead of reaction to alarms, in remote surveillance cameras, access control and other systems are monitored as in a control room, but from a different location. This is useful if maintaining a fully equipped, control room or having an operator on location at all times is too expensive or unnecessary. Remote surveillance operators inform e.g. guards or client contact personnel of their observations, who then perform the proper response. They can also handle any customer service functions that are not necessary to complete on location, such as after-hours door phones and other individual access requests.

2.5. Personal protection

Personal protection, also known as *body guarding*, is a very specific line of work that requires great expertise. It also requires a lot of resources if continuous, considering the long work hours and the need to accompany the protected person at all times. As it is with all guarding services, personal protection is or should not be a sign of status, but rather a risk management method. Constant around-the-clock protection is less common than situation-based protection; a certain, temporary need might be for example a credible threat on a person's health and life which then requires protection until the matter is settled. Another example might be a public appearance, where the threats are more likely due to the crowd and predetermined schedules; in these situations, personal protection is then used or enhanced temporarily. Personal protection is not necessarily attached to a certain person or persons that are under protection, but sometimes to the threat itself; this type of situation can come up in e.g. healthcare, if a particular patient poses immediate threat to all attending staff. In this type of situation, the guard stays with the patient while protecting the staff.

The basic goal of personal protection is to get the protected persons to safety in all situations. This is achieved by both immediate intervention to the threat as well as escaping the situation. Heroics when facing threats are not enough though; analysing the risks and anticipating the threats beforehand are also critical. This means prevention and preparedness including e.g. cooperation with authorities, scouting locations beforehand, getting equipped properly and such play a big part. In order to accomplish all this, personal protection requires forethought as well as great mental and physical acuity.

2.6. Cash and valuables transport

Cash and valuables transport refers quite obviously to a service where valuables are transported from one location to another. The details however are more important than this basic premise shows. For the client in banking or retail, this removes the risky task of transporting cash on their own, thus removing themselves from the possible physical threat that may follow. Proper guarding services deter theft attempts very well, especially considering the special equipment that is provided from vehicles to carrying cases by the company. In addition, once the valuables are handed over (with proper receipts and bookkeeping of course), they also become financially liable for them. This removes also the financial risk from the client, as any loss after this point is compensated by the guarding service, or rather their insurance carrier.

In case of some unique valuables, the transport itself must be discreet which require different tactics. As a whole however, this serves the same purpose as more common cash transports – to deter crimes and to transfer the remaining risk towards a competent guarding service. The personnel working in these duties often need to have special training, often mandated by insurance carriers. If trained guards are not of a big enough deterrence and an attempt on the transported goods are made, the main function of the guards is to prevent further damage to themselves and the surroundings. The risk of running into professional, perhaps even quite ruthless perpetrators is real and the preservation of life always comes first.

2.7. Stewards

Stewards are a special branch in private security, so much so that they are sometimes not even considered as part of guarding services. The main task of stewards is to maintain order, safety and security in public locations such as shopping centres and public transportation, as well as events like festivals, shows, concerts and conferences. Though the overall role in safety & security risk management still applies, stewards are less concerned with physical security of premises like most guard services, but more with crowd management. This task usually requires special rights, as the necessity to interfere with the basic rights and liberties of people comes up relatively often.

In public buildings where physical security is still a great concern, stewards act in a manner very similar to static guarding services, maintaining and complementing structural security and technical surveillance in addition to surveying public order. However, with the on-and-off or fleeting nature of public events, steward services move from one working location to another. Events requiring steward services are considerably more common in the summer and in weekends, often with relatively short hours. This means that demand for the service in an area fluctuates greatly.

Because of the crowd management-nature of the task and varying demand, national legislations usually allow stewards to be used on a temporary basis and/or with very little training, while at the same time giving extensive special rights to them. This has been addressed by having different levels of stewards; temporary stewards with less rights that can be used in most tasks, and professional stewards with more extensive rights than can handle more demanding crowd management situations. It is therefore crucial to balance the steward staffing correctly, not relying only on the total number.

Finally, it is important to note that stewards have the moral responsibility and even legal requirement to prioritize the safety of the crowd above all else.[112] This translates to training and guidelines for the prevention and mitigation of a wide variety of risks; considering the priority of the safety of the crowd, arguably the most critical skills are then in managing risks that either have the potential to injure several people at once, and/or might cause a

[112] Private Security Services Act 1085/2015 (Finland), (Laki yksityisistä turvallisuuspalveluista 1075/2015), adopted 1.1.2017, published by *Finnish Ministry of Justice*. Retrieved from https://www.finlex.fi/fi/laki/ajantasa/2015/20151085

panic or stampede. Therefore, the prevention and deterrence of violence, terroristic attacks, fires and accidental explosions (such as those from gas bottles or pyrotechnics) are of the utmost importance. In mitigation, the ability to assist in swift but safe emergency evacuation is important. These, in addition to all other required skills, make steward services crucial for events and public locations that want to safeguard their customers in all situations.

3. Legislation concerning guarding services

3.1. Latvian legislation

(author Uģis Začs)

There is a broad range of guarding and security services offered in Latvia. Guarding and security services in Latvia are regulated by the Law on Guarding Activities. The Law on Guarding Activities defines the following types of guarding services:

1) Installation of technical guarding systems;
2) Physical guarding service;
3) Technical guarding service;
4) Cash-in-transit guarding service.[113]

In order to commence any of the guarding services, a commercial operator engaged in guarding must receive a special permit (licence). Each of the special permits (licences) specifically indicates those guarding services that the commercial operator who has received the permit (licence) is permitted to offer. In Latvia, special permits (licences) are issued by the State Police and the permit is valid throughout the territory of the country.

[113] Apsardzes darbības likums. Adopted on 13.02.2014. *Latvijas Vēstnesis,* 06.03.2014, No.37., Latest amendments 19.01.2017., Article 3

The Cabinet of Ministers establishes the requirements for obtaining the special permit (licence) and the requirements, which must be met during the period of validity of the special permit (licence). The Cabinet also establishes the procedure of issuing the special permit (licence), its duplicate or a reissued special permit (licence) to the commercial operator, the annulment procedure of the special permit (licence), as well as establishes the amount of state duty payable for issuing of the special permit (licence), its duplicate and a reissued special permit and the payment procedure.[114]

Each specific permit (license) defines a set of specific security and guarding services permissible to be performed for each type of guarding service.

Installation of technical guarding systems

A commercial operator, which has received a permit (licence) on the installation of technical guarding systems may perform services related to designing of technical guarding solutions, installing and servicing of technical guarding systems, as well as providing consultations on the corresponding issues.

Physical guard service

A commercial operator, which provides physical guarding service, may provide it for various types of objects under the condition that a security staff member is located at the protected object or in its direct vicinity or arrives at the protected object upon request by the recipient of the guarding service, a member of the security staff or another person. Physical guarding involves the

[114] Apsardzes darbības likums. Adopted on 13.02.2014. *Latvijas Vēstnesis*, 06.03.2014, No.37., Latest amendments 19.01.2017., Article 6

guarding of real estate, goods or other movable property, escorting of cargoes or other items of material value (except cash-in-transit guarding service), guarding of a physical person (bodyguard service), providing of internal order and security at the protected object and defending of physical persons at the object as well as providing consultations on the corresponding issues.[115] Objects eligible for providing physical guarding can be most different, including stores, shopping centres, offices, banks, factories, et.al. Physical guarding is provided also at various events. In Latvia, bodyguard service is also defined as a physical guarding service. In order to provide bodyguard services, a commercial operator does not have to apply for a special permit (licence). Physical guarding services are often used for the control and monitoring of internal operational processes of companies.

Technical guarding service

A commercial operator provides the technical guarding service of an object by using a guarding control centre equipped with a monitoring and alarm signal reception remote device (hereinafter – guarding control centre), which receives a signal from the technical system installed at the protected object for the purpose of ensuring continuous operation of the guarding control centre as well as an immediate arrival of the mobile group of the security staff at the protected object after receiving information (alarm signal) from the guarding control centre.[116] Depending on client's wishes, the guarding service market offers technical guarding solutions for separate personalised services:

[115] Apsardzes darbības likums. Adopted on 13.02.2014. *Latvijas Vēstnesis*, 06.03.2014, No.37., Latest amendments 19.01.2017., Article 3

[116] Ibid

1) **call service** – in the case of receiving an alarm signal, a member of the guarding control centre staff does not deploy the mobile group, but contacts the contact person designated by the client by phone and informs about the reception of the alarm signal. The client has the right to make a decision on sending a mobile group of security guards or the client himself/herself inspects the cause of the triggered alarm;
2) **information forwarding service** – upon receiving an alarm signal, the system installed at the guarding control centre automatically sends information to the client about the alarm triggered at the protected object or the guarding control centre staff member sends information to the client on the triggered alarm manually. After that, the client makes his/her own decision on further action.

The main difference between the technical guarding service and the physical guarding service lies in the fact that the technical guarding service provides guarding of an object by technical means, various systems and devices, which, once triggered, provides that the object is visited by the commercial operator's mobile group or the client is informed by the triggered system. Physical security staff stays directly at an object.

Cash-in-transit guarding service

Cash-in-transit guarding service is a security, guarding service involving transportation of money. Cash-in-transit guarding service can be divided into four stages:

1) **Stage 1** – collection of cash, collection from the client, client's object or from a specialised equipment;

2) **Stage 2** – transportation of cash to a specialised cash processing object;
3) **Stage 3** – processing of cash – counting, verification;
4) **Stage 4** – storing of cash, transfer to the bank account provided by the client.

For cash-in-transit guarding service, guarding service commercial operator uses guarding control centre, which continuously follows the location of the cash-in-transit vehicle by means of a global positioning system. The centre regularly communicates with the security staff members engaged in cash-in-transit guarding service. Cash-in-transit guarding service also includes providing of consultations on the corresponding issues.[117]

By performing one of the aforementioned guarding services the guarding commercial operator also has the right to provide consultations in specific areas. To perform security audits, to develop a security concept, to draft regulations, instructions and to perform control operations.

Detective activities

Currently, the detective activity in Latvia has been separated from the guarding services. Detective activity in Latvia is regulated by the Law on Detective Activity. According to the Law, detective activity involves contractual services provided by individual commercial operators, partnerships and companies (hereinafter: detective company) and certified persons (hereinafter: detective) to a physical, or legal entity for the purpose of protecting its rights and

[117] Apsardzes darbības likums. Adopted on 13.02.2014. *Latvijas Vēstnesis*, 06.03.2014, No.37., Latest amendments 19.01.2017., article 3

lawful interests. A detective company and a detective can provide the following detective activity services:

1) to gather information in civil and criminal cases;
2) to search for persons who have committed offences against the law or for missing persons;
3) to ascertain facts, items or persons related to illegal activity;
4) to provide consultations to physical and legal persons on security issues;
5) to clarify facts related to unfair competition, illegal commercial activity or other illegal business activity;
6) to collect information characterising a person before signing an employment contract or another type of contract involving civil liability or information on person's solvency;
7) to verify information related to the fulfilment of an insurance contract and compensation of material loss;
8) to search for the lost or illegally confiscated property of physical and legal persons.[118]

A detective company and a detective can also provide other services if they are consistent with the law and serve the goals, defined in Part 2 of this article.

3.2. Lithuanian legislation

(author Stanislav Dadelo)

In Lithuania the Law On Private Security IX-2327 as last amended on 29 June 2017 No XIII-537[119] (henceforth referred to as

[118] Detektīvdarbības likums. Adopted on 05.07.2001. *Latvijas Vēstnesis*, Nr. 110 (2497), 20.07.2001., Latest amendments 14.06.2012, Article 2

[119] Law on private security. 8 July 2004 No IX-2327. As last amended on 29 June 2017 No XIII-537. Vilnius

the "Act" in this chapter). This Act regulates the general conditions of private security as licensed activity, the conditions/grounds for issuing licences, the rights and duties of security guards, security staff and trainee security staff engaged in private security, the cross-border transport of cash by road, the conditions of lawfulness of the use of physical coercion and firearms in carrying out private security operations and state supervision of such activity.

Private Security Services include:

Chapter I	General provisions (purpose of the law and definitions)
Chapter II	Requirements for persons engaged in private security operations, their rights and duties
Chapter III	Licensing framework of private security
Chapter IV	Bases for carrying out licensed activity
Chapter V	Organisational framework for private security
Chapter VI	Use of physical coercion and firearms
Chapter VII	Final provisions (supervision of private security, and disputes concerning infringements of this law, and liability for infringements)

The final bullet point is important to note as somewhat an Act general definition, considering the terminology:

1) security guard shall mean a natural person pursuing individual activities who has acquired the right to provide private security services to clients in accordance with the procedure laid down in this Law;
2) member of security staff shall mean a natural person protecting persons and property who is employed by a security guard or a security company;

3) trainee member of security staff shall mean a natural person seeking to work as a member of security staff who is employed by a security guard or a security company and assists a member of security staff in protecting persons and property;
4) security company shall mean a legal person, another organisation or a division thereof entitled to engage in the activity to in this Law;
5) head of security staff shall mean a natural person responsible for compliance with the conditions of licensed activity of a security company;
6) private security shall mean activities aimed at safeguarding the regime at a protected facility, protecting from attempts on the life and/or health of natural persons as well as property of natural and/or legal persons.

This act focuses on guarding activities. According to the Act, providing guarding services on the basis of client contracts for the purpose of earning income requires a private security trade permission to carry out activities which can be obtained by a private (security officer certificate) or legal (license) person. The licence application is approved by the National Police Service, with possible conditions and limitations. The personal situation of the applicant or members of its governing body (at least 18 years old, adequate health and reputation). Offering guarding services without a license is a criminal offence.

The security process is according to the protected object regime. Safeguarding of the regime shall mean the actions of a security guard or a member of security staff whereby he maintains public order at a protected facility and/or ensures compliance with the rules established by the owner or manager of the protected facility. An institution authorised by the Government of the Republic of Lithuania may prohibit the private security operations specified in this Act where they might pose a threat to the national or public security or public order.

Private security services are bound by some specific responsibilities laid down in the Act.:

1) immediately inform the police when it is suspected that an administrative offence or a criminal act is being planned, is being committed or has been committed;
2) where an administrative offence or a criminal act has been committed at a protected facility or against a protected person, secure the site of the incident and take measures to identify witnesses;
3) provide assistance to persons detaining the suspected offenders to the extent that it does not interfere with their actual duties;
4) having used a firearm or physical coercion, provide, if necessary, medical first aid to the victims;
5) immediately inform the police about the use of the firearm or physical coercion where it resulted in the death of a person or impairment of his health or caused damage to his property;
6) when making his way to the site of the incident due to the triggered alarm at protected facilities in which electronic security is in place or to provide assistance to other persons and members of security staff engaged in private security operations, also during cash/valuables-in-transit operations, switch on the flashing orange light of the vehicle;

7) wear clothes with the clearly visible name and distinctive signs of the security company or clothes with the word 'Security'. During international events at which private security operations are carried out, clothes with inscriptions in foreign languages may be worn. This requirement may be omitted where a specific natural person is being protected or in the course of the cross-border transport of cash by road from one participating Member State to another under the conditions laid down in Regulation (EU) No 1214/2011;
8) upon the expiry of his security staff certificate, immediately return the security staff certificate to the granting authority.

3.3. Finnish legislation

(author Kaci Bourdache)

In Finland, the Private Security Services Act 1085/2015[120] (henceforth referred to as "Act" in this chapter) and all decrees issued under it governs the whole private security sector. The purpose of the Act is to ensure the quality and reliability of private security services, as well as to promote cooperation between them and the authorities. Private Security Services include Guarding services (services described in chapters 1.3.1.–1.3.6.), steward services (services described in chapter 1.3.7.), which are further divided into common stewards and stewards assisting police or Border Guard and finally security services, which include the planning, installation, repair or alteration of structural protection or of electronic monitoring systems, and the planning of other security arrangements.

[120] Private Security Services Act 1085/2015 (Finland), (Laki yksityisistä turvallisuuspalveluista 1075/2015), adopted 1.1.2017, published by Finnish Ministry of Justice. Retrieved from https://www.finlex.fi/fi/laki/ajantasa/2015/20151085

"Security services" is important to note as somewhat of an anomaly, considering the terminology. Typically, "security services" are understood to include all services above, in addition to, for example, consulting services. In Finnish legal terminology however, the above three are completely separate, with other security services not being considered by law at all. Keeping this distinction in mind is important; however, this article focuses on guarding services and we will proceed with concepts related to that. Steward services are admittedly often though intertwined with guarding services, and they are discussed when necessary.

According to the Act, providing guarding services on the basis of client contracts for the purpose of earning income requires a private security trade licence which can be obtained by a natural or legal person. The licence application is approved by the National Police Board, with possible conditions and limitations. The personal situation of the applicant or members of its governing body (at least 18 years old, known to be suitable) is considered, as well as the sufficiency of its assets. Offering guarding services without a license is a criminal offence. It is therefore important to understand the limitations; specifically, it is legal to arrange guarding by direct hiring, because in this case there is no client contract involved. In that case however the guards operate under general rights and responsibilities that apply to all people. It is also legal to offer guarding services pro bono, as then there is no purpose to earn income. In any other circumstance a private security trade licence holder must be used.

According to the Act, guarding means the guarding of property, protection of personal inviolability, uncovering of crimes concerning a person or object under guard or the client, and supervision of such assignments. It is specifically mentioned that suppliers may not accept contracts which include a commitment to maintain public order and safety, as that is considered the task of accountable public authorities, namely the police.

Private security services are bound by some specific responsibilities laid down in the Act. One such is a special confidentiality requirement concerning confidential security arrangements, business or professional secrets or privacy of any party to the contract. Guards and stewards must write action reports at least every time they apprehend a person or they had to use force to fulfil their duty. Most importantly, the general principles must be applied in all situations: Guards must carry out their assignments properly and impartially, and promote a conciliatory spirit. Guarding shall be carried out without causing more damage or harm than is necessary to do the job. In guarding, nobody's rights may be interfered with more than is necessary in order to do the job. Action taken in carrying out the job shall be justifiable in relation to the importance and urgency of the job and to the situation as a whole. Furthermore, guards must inform any person who is the target of the action the grounds of that action.

The previous chapters are an overview of the legislation that concerns the private security industry as a whole in Finland. For more detail, the table in the next page collects rights and requirements of the Act to one simple presentation. It explains the following: where this type of service can operate, what is their role, what permits are needed to make use of that service, from where can they be legally obtained, what insignia they must wear or carry, and finally what legal rights they have to fulfil their role. For this final point, it is important to note the general requirements like the general principles which were discussed above.

Table 4

Private Security actors in Finland (Private Security Services Act 1085/2015)

	Security guards	Security stewards (assisting police or Border Guard)	Security stewards
Operates	Anywhere	Healthcare, social service-, social insurance- and employment offices, shopping centre, public transportation, ports, airports, refugee centers	Public meetings, public events, private events, camping grounds, passenger vessels, hotels, restaurants, universities
Role	Guarding property, personal protection, uncovering crimes	Maintaining order and security and preventing crime and accidents	
Permit to use	No permits needed. Personnel must have guard certification	From local police. Personnel must have steward certification and guard training	No permits needed. Personnel must have steward certification
Where to get	Licensed private security companies		Licensed private security companies, or direct hiring
Insignia	Uniform (except: cash and valuables transit, personal protection, uncovering crimes), guard identity card	Uniform, steward identity card	Safety vest or badge, steward identity card
Rights	Apprehending suspects of certain crimes. Prevent entry and remove threatening or unauthorized person(s) from the premises. Frisking apprehended persons. Forcible means.	Apprehending suspects of certain crimes. Remove a person that disturbs others, acts in a threatening or violent manner, endangering security; or is in an area closed from the public. Apprehend a person if removal is insufficient. Frisking apprehended persons. Forcible means.	ALL MENTIONED ON THE LEFT, plus: Prevent entry based on intoxication, behaviour, earlier behaviour, equipment, access limited by law or owner/operator; perform security checks at access points.

Conclusions

The guarding services in most countries are regulated by law, and are an effective option to provide and maintain security and safety for objects and people. One of the most important things is that guarding services provide specially trained and equipped security personnel with special rights. If security services answer the needs of their client base, they provide a multitude of options to manage various security and safety risks, not only in the domain of physical security but in e.g. emergency preparedness, information security and occupational safety as well.

Managing safety and security risks in an organization is often simpler if they are conceptualized into different elements, such as information security, occupational safety, cybersecurity, emergency preparedness, physical security and environmental safety. The elements often intersect in practice, but managing risks in each domain with the proper resources is vital.

To select a needed security and safety service and partner who will provide it, it's important to identify the risks of the organization and to fully understand the legislation of the country in which guarding service is needed, as well as that it is in the end a financial decision, one that should not be done lightly.

References

Johnson, B. & Ortmeier, P. (2018). *Introduction to Security, Operations and Management*. Pearson Education

Halibozek, E. & Kovacich, G. (2017). *The Manager's Handbook for Corporate Security*. Elsevier Inc

International Organization for Standardization (2018). ISO 31000:2018

Ricks, T. & Ricks, B. & Dingle J. (2015). *Physical Security and Safety, a Field Guide for the Practicioner*. Boca Raton: CRC Press

van Steden, R. (2007). *Privatizing Policing, Describing and explaining the growth of private security*. BJU Legal Publishers

Zalud, B. (2010). Tech-Armed Officers on Future's Watch, *Security in 2020*. ASIS International

Private Security Services Act 1085/2015 (Finland), (Laki yksityisistä turvallisuuspalveluista 1075/2015), adopted 1.1.2017, published by Finnish Ministry of Justice. Retrieved from https://www.finlex.fi/fi/laki/ajantasa/2015/20151085

Apsardzes darbības likums. Adopted on 13.02.2014. *Latvijas Vēstnesis*, No. 47 (5107), 06.03.2014., Latest amendments 22.12.2016.

Detektīvdarbības likums. Adopted on 05.07.2001. *Latvijas Vēstnesis*, No. 110 (2497), 20.07.2001., Latest amendments 14.06.2012.

Law on private security. 8 July 2004 No IX-2327. As last amended on 29 June 2017 No XIII-537. Vilnius

About the Authors

Kaci Bourdache, Senior Lecturer
MBA in Security Competence
Senior Lecturer of Safety, Security and Risk Management (5 yrs), Chief Fire Inspector for City of Helsinki (4 yrs), Private Security and related training (10 yrs)

Uģis Začs, MBA
Uģis Začs received a Master's Degree in Business administration at the Riga Business School in 2015 and Bachelor's Degree in Regional development and governance at the Latvian University of Agriculture in 2011.
The author works in one of the largest security company in Baltic States – SIA GRIFS AG – since 2006. The author works as a corporate client security manager and in his daily life deals with physical and technical security, manages different kind of objects, develops security concepts, and controls the security status of facilities. The author is also a lecturer at Turiba University, the programme on Company Security.

Stanislav Dadelo, *prof. Dr.ph.*
Vilnius Gediminas Technical University
Mr. S. Dadelo brings more than 25 years of professional work experience in various internal affairs of Lithuania and private security areas including security staff training. Author of the scientific monograph "Factors Determining of Competences Lithuanian Security Workers". Creators of bachelor's study program "Security systems engineering" in Vilnius Gediminas Technical University. Member in editorial boards of six scientific journals. Science and practice internships in Sweden, French, Denmark, Malta, Portugal, Germany, Poland, Check Republic, People's Republic of China etc.

RELATIONSHIP OF RISK AND QUALITY MANAGEMENT

Tuomas Wuorikoski

Introduction

This article reveals the relationship between risk and quality management. For the reader, it is recommended to familiarize fundamental concepts of risk and quality management prior to reading this article, because definitions of those are not included in this article or book. This article emphasises the background, challenges and applications of risk and quality management.

1. Risk and quality management

1.1. Concepts

There are various definitions regarding risk, quality, risk management and quality management. In this article, the definitions are based on standards published by International Organization for Standardization (ISO). According to ISO 9000:2015 "The primary focus of quality management is to meet customer requirements and to strive to exceed customer expectations". [121] This commonly used definition clearly includes quality management to be a crucial element of organisations' success in all levels from strategic results to operational performance.

[121] ISO 9000:2015 Quality management systems. Fundamentals and vocabulary. Retrieved from https://www.iso.org/standard/45481.html, 2.3.1.1

Likewise, with the definition of quality management, there are several definitions for risk and risk management. ISO 9001:2015[122] defines risk to be "effect of uncertainty" and ISO 31000:2018 specifies the definition to be "effect of uncertainty on objectives".[123] ISO 31000:2018 states that the deviation from expected can be negative and/or positive and might lead to opportunities and threats.[124] Risk management is defined to be "coordinated activities to direct and control an organization with regard to risk".[125]

1.2. The relationship of the concepts

When comparing the presented definitions, it is clear that risk and quality management are intertwined together. However, it is worth mentioning that both concepts refer to comprehensive actions of any organisation in all of its levels, not only to the quality of security operations or security risk management, despite that this books itself focusing to security. It is a common misunderstanding that these concepts would consider organisations narrowly only from some sub-category point of view.

Both are looking at organisations' success from same, but still different angle. The same angle is that to be able to actually define these in organisation's context, one must first understand the operations, objectives, operational environment and most importantly, when and how organisation succeeds. On the other hand, the quality's essence is the success factors, while the risk's essence is the positive and negative

[122] ISO 9000:2015 Quality management systems. Fundamentals and vocabulary. Retrieved from https://www.iso.org/standard/45481.html, 3.7.9

[123] ISO 31000:2018 Risk management. Guidelines. Retrieved from https://www.iso.org/iso-31000-risk-management.html, 3.1.

[124] Ibid

[125] Ibid, 3.2

uncertainties. It is fair to define that managing risks and quality is the paradox of success, there will not be one without the other.

2. Requirements for risk and quality management

2.1. Compliance requirements

It is typical that legislation does not require holistic approach to risk and quality management. In the member countries of the European Union, there are usually industry or risk context specific requirements for risk and quality management. Industry specific means e. g. that government agencies are due to ensure a certain level of risk and quality management in all conditions from business contingency point of view, social and healthcare sector's operators are required to ensure safety of customers and patients, traditional industry is due to ensure a certain level of risk and quality management of the actual production process. Risk context specific requirements mean e.g. ensuring a certain level of risk and quality management of risk contexts of safety of products and services, occupational safety, condition of premises, privacy and environmental issues. Overall organisations should have awareness of different compliance requirements they are under when operating in a certain field of industry or in a certain operational environment, which is from legislative point of view an obvious issue, but also one of the ground level requirements of each ISO standard.

The ISO standards follow the same principles, providing tools and methods mainly for risk specific risk and quality management and it is typical for organisations to certify this type of standard to be the most significant focus area of the organisation's risk and quality management. However, since there are also comprehensive standards like ISO 9001:2015[126], ISO 9004:2009[127] and ISO 31000:2018[128], many organisations build their risk and quality management for more holistic ground. It is worth mentioning that ISO standards are formed in accordancewith same high level structure since 2012, which means that risk management is included to be part of each quality management standard, despite the focus area of that standard. That is a strong statement of the relationship between risk and quality management.

2.2. Holistic or context specific approach?

The requirements for systematic and holistic risk and quality management rise typically outside the legislative requirements. In most cases, it rises from either internal understanding of its significance or external requirement from customers, owners or partners. The risk of too narrow and context specific risk and quality management is that organisation is not able to understand key factors of success or possible uncertainties of the main objectives and operations. The significance to success will be presented later in this article.

The holistic standards mentioned above enhance that risk and quality management is taken into account in all levels and operations of an organisation. This means that these should be an integrated part of everyday operations in all levels of organisation. If the organisation hold significant risks in some context, e.g.

[126] ISO 9000:2015 Quality management systems. Fundamentals and vocabulary. Retrieved from https://www.iso.org/standard/45481.htm

[127] ISO 9004:2009 Managing for the sustained success of an organisation. A quality management approach. Retrieved form https://www.iso.org/obp/ui/#iso:std: iso:9004:ed-3:v1:en

[128] ISO 31000:2018 Risk management. Guidelines. Retrieved from https://www.iso.org/ iso-31000-risk-management.html

environmental hazards, it is recommended and usually required by legislation to have additional effort in risk and quality management of that context. In this case, context specific risk and quality management programs and standards bring additional value to the organisation. It is still important to ensure that all risk and quality management actions are balanced to be holistic in order to avoid that some context would have too significant importance, which could lead to underperforming in other contexts.

3. Best practices

3.1. Integration

ISO 9001:2015, 9004:2009 and 31000:2018 all enhance the integration of risk and quality management together, but also integration into all levels and operations of an organisation. Understanding the key success factors, ensuring the proper actions in order to achieve the objectives, avoiding uncertainties and utilising opportunities sounds something considered self-evident. However, integrating all these together is one of the biggest challenges of risk and quality management. It is typical that people interpret the concepts and procedures according their own understanding, beliefs and values. One success factor in this sense is to create a common understanding of risk and quality management procedures.

If there is no true integration, the organisation is not able to develop risk and quality management systematically, the results are not comparable and the organisation is not able to define success factors, phenomena to avoid and opportunities to seek. This most likely leads to unproductive risk and quality management, which is a more or less irrelevant part of operations and is usually seen as a frustrating and superimposed process. Standards mentioned above enhances best practices on how to integrate risk and quality management holistically.

As one of the most important elements in a journey to integrate risk and quality management into operations, is to define objectives in everyday business. Once again, a self-evident sounding issue is one of the most difficult ones. This means that an organisation should be first able to define the objectives of the organisation as a whole (strategic objectives) and from each operations point of view (operative objectives) with measurable definitions of key performance indicators. The second phase is to define how and with what kind of operations/processes, competences, machines/tools and systems e.g. the organisation will achieve the objectives. The third phase is to understand not only the possible negative uncertainties and how to avoid and mitigate those, but also the possible positive uncertainties and how to utilise those. If this sounds self-evident to you, you might want to try to define those from your own organisation's or personal life's point of view. The fact is that if you are not able to define the requirements presented in this paragraph, you are not able to manage risks and quality systematically and with a holistic approach.

3.2. Business development

It is a difficult and often bureaucratic path, trying to integrate a holistic approach to risk and quality management, when the origin to this arises from compliance requirements. The challenge usually is, as stated before, that it leads to unbalanced entity or no entity at all. Excellent organisations understand the analogy between objectives, means how to reach those, phenomena to avoid and opportunities to seek. One of the most powerful methods understanding this is scenario based methods, e.g. from a strategic point of view blue ocean strategy tools and back casting and in process level different scenario analysis. Scenario methods forces participants to truly understand and analyse the operations with understandable and context specific outcomes.

The EFQM Excellence model defines that "Excellent Organisations achieve and sustain outstanding levels of performance that meet or exceed the expectations of all their stakeholders".[129] The model and its requirements are based on the knowledge from excellent organisations, which can be defined to be "excellent organisations" according to EFQM assessments. The model enhances (EFQM Excellence Model 2013, Fundamental concepts) that understanding and creating organisation's future is more and more crucial in rapidly developing business environment. If the organisation does not have systematic procedures in this, they are able to utilise and create few opportunities comparing to excellent organisations. Risk and quality management is part of business development and continuous improvement, or at least those should be, whether it is about every day development or future thinking.

3.3. The future of risk and quality management

Trends are shaping operational environment faster than ever and organisations are facing opportunities and uncertainties, which have never existed before. The global megatrends are related to e. g. changing world order and economic power, environmental crisis, individualism and new ways of working, digitalization (inc. robotics, artificial intelligence and Internet of Things), demographic change and technological convergence. All of these will have an effect globally and to any field or sector of industry. Trends have shaped the future before, but one significant difference is the huge

[129] EFQM Excellence Model (2013). Retrieved from http://www.efqm.org/

influence and unpredictability of change. This enhances the role and significance of risk and quality management in the future and makes it an even more crucial success factor than now.

Conclusions

1. Risk and quality management are significant success factors to any organisation and there cannot be one without the other.
2. Risk and quality management must be an integrated element of operations, which can be done only if the organisation is able to define objectives (understanding the organisation), define how to reach those (quality management), phenomena to avoid and opportunities to seek (risk management).
3. Megatrends are shaping the future more than ever and that increases the significance of risk and quality management.

References

EFQM Excellence Model (2013). Retrieved from http://www.efqm.org/

ISO 9000:2015 Quality management systems. Fundamentals and vocabulary. Retrieved from https://www.iso.org/standard/45481.html

ISO 9001:2015 Quality management systems. Requirements. Retrieved from https://www.iso.org/standard/62085.html

ISO 9004:2009 Managing for the sustained success of an organisation. A quality management approach. Retrieved from https://www.iso.org/obp/ui/#iso:std:iso:9004:ed-3:v1:en

ISO 31000:2018 Risk management. Guidelines. Retrieved from https://www.iso.org/iso-31000-risk-management.html

About the Author

Tuomas Wuorikoski, Development manager
MBA in Entrepreneurship and Business competence. Organizations' strategic and operational planning, development and management both in a general level and the areas of quality, risk management, business continuity management & security and safety.

PUBLIC-PRIVATE SECURITY PARTNERSHIP

Raimundas Kalesnykas

Introduction

Trends of threats and challenges for European societies, which have taken place in the recent years, have also changed the system of subjects in charge of security. Due to limited financial resources today sees the incapacity of the Member States public authority to guarantee proper level of security to the people, which is in particular in relation to the protection of business entities. In the face of criminal risks and threats, large numbers of business companies turn to alternatives either by taking care of their own security or by purchasing security services. Private policing[130] and/or private security leading above-mentioned process and spontaneously developing alongside with community policing.[131]

This article raises a hypothesis that in a democratic society and free market economy private resources may be employed in security area, whereas the efficiency largely depends on the competitiveness of security organizations as a whole. Nowadays public and private security organizations interacting together play the major role in security market. The phenomena of *public-private security partnership* (hereinafter – PPSP) is obvious and is promoted

[130] Button, M. (2002). *Private Policing*. UK: Willan Publishing;
Johnston, L. (2005). *The Rebirth of Private Policing*. London: Routledge

[131] Brogden, M., Nijhar, P. (2013). Community Policing. UK, London: Routledge;
Miller, L. S., Hess, K. M., Christine, H. (2017). Com*munity Policing: partnerships for problem solving*. USA, Boston: Cengage Learning

as providing a synergetic effect in solving problems of (in)security.[132] Many Member States are not familiar with the concept of security partnership and institutional forms of partnership in the area of security and crime prevention and looking for the theoretical justification of PPSP. For example, Finland, Denmark, Norway, Sweden, the United Kingdom and the Netherlands play a leading role using PPP model in security area.

Security environment has changed from one dominated by a state funded "public" police, to one in which the provision of security is shared between public and private actors. Private security has expanded to meet citizen demand, and increasingly governments are turning to the private sector to provide security services that are more flexible, cheaper, and in some cases more specialised than which can be achieved by the police and other public security forces.

Private security companies play an important role in reducing and preventing crime, managing security risks and providing security services in a proportionate manner. The exponential growth of private security worldwide has unleashed debates across disciplines concerning state sovereignty, legitimacy and authority in the public police domain. In analysing the partnership between public and private security bodies, the majority of the literature employs a model that emphasises either a competitive or a collaborative relationship.[133] According to J. Berg[134], private security companies assist the police by functioning as their eyes and ears and supporting the public

[132] Prenzler, T., Sarre, R. (2012). Public-private crime prevention partnerships. In book: Prenzler, T. *Policing and security in practice: challenges and achievements*. UK: Palgrave Macmillan, pp. 149–197

[133] George, B., Button, M. (2000). *Private Security*. UK, Leicester: Palgrave Macmillan

[134] Berg, J. (2007). The accountability of South Africa's private security industry: mechanisms of control and challenges to effective oversight. Newlands, South Africa: Criminal Justice Initiative of the Open Society Foundation for South Africa.

security agenda, or a competitive and perhaps hostile relationship emerges, where the private security sector encroaches on the state police's domain. Research analysis highlighted three major developments, which have significantly affected PPSP – globalisation, marketisation, democratization.

Such research methods as scientific literature and document analysis on security industry development in EU, comparative analysis on legal requirements for public-private security partnership, content analysis of identifying the reasons and risks implementing public-private partnership tool in security industry and doctrinal analysis of establishment of the new form of guaranteeing security in the organization and states were used in this article. Research results can be used both in a theoretical way and in practise in order to understand problems arising in the implementation of public-private security partnership model and provide simple ways of solving them. The author in this article explores the trends of security market development and factors that shape the various reasons of relationships developed between the private security industry and the public security bodies. The ultimate efficiency of the PPSP might be achieved when powers and competence of the two is properly balanced. As well, the author draws a critique attention of the lack of legal regulation on the accountability issue in PPSP within Member States and the need for a re-think of how this phenomenon can be used better and how the partnership can be held accountable and transparent.

1. Phenomena of public-private security partnership

Progress of society development and the latest technology "revolution" are particularly affecting the development of effective national security systems among Member States. From this point of view, ongoing discussions[135] about current threats, risks and insecurities that emphasise the need for further research in this field, and additional development of partnerships between the private and public sectors in the field of security are essential.

Analysis of PPSP development in EU shows, that is no universal scenario of how to create a successful PPSP model and what works perfectly in one Member State can be tricky and challenging in another. That is mainly because of the security cultural differences and the fact that the general relation between public and private security sectors differs amongst Member States. In some EU countries, formality is the most important part of PPSP, while in the others pragmatism is more important. Today PPSP in on the agenda of EU and Member States governments today and presents a strong policy option for legislation of such phenomena development.[136]

1.1. Definition of public-private security partnership

The present emergence and demand for public-private partnerships within security is a new phenomenon and a unique concept

[135] Sotlar, A., Meško, G. (2008). Police and private security in Slovenia – between conflict, competition, cooperation and partnership. CRIMPREV Symposium "Private policing and security – relationships between the private and public sectors", Ljubljana, University of Maribor, 4–6 December 2008, pp. 7–8. Retrieved from https://www.fvv.um.si/crimprev/abstracts.pdf

[136] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union. *Official Journal of the European Union*, L 194/1 (19.7.2016). Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?toc=OJ:L:2016:194:TOC&uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG/ Communication from the Commission to the European Parliament, the Council and the European Economic and Social Committee "Security Industrial Policy Action Plan for an innovative and competitive Security Industry", COM/2012/0417 final (26.7.2012). Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2012:0417:FIN

to the system of criminal justice and law enforcement. Conception of PPSP is being changed by substantial changes in the European societies, political and economic instability in the "exposed countries", the emergence of new forms of property, a wide range of security market players and a rapid development of private business.

PPSP have no single definition. T. Prenzler and R. Saare views them as relationships built on security partner needs, capabilities, and two-way communication.[137] C. P. Nemeth refers to them as contractual arrangements in which resources and capabilities are shared.[138] And for M. K. Sparrow, public-private partnerships are either organized efforts with institutional support and written agreements, or informal collaborations.[139]

PPSP must be publicly accessible, dedicated, resourced, engaged, legal and sustainable. From this point of view, PPSP can be defined as arrangements between public (government) and private security sector entities for the purpose of providing security infrastructure, community security needs and related security services. Such partnerships are characterized by the sharing competences, risk, responsibility, results and reward between the partners. It is important to note that public agencies that contracted with the private sector to fulfil security services as well as instances of funding or granting opportunities are not examples of PPSP and can perhaps be classified or studied under the umbrella of different

[137] Prenzler, T., Sarre, R. (2012). Public-private crime prevention partnerships. In book: Prenzler, T. *Policing and security in practice: challenges and achievements*. UK: Palgrave Macmillan, pp. 149–197

[138] Nemeth, Ch.P. (2012). *Private Security and the Law*. USA: Elsevier, pp. 139–140

[139] Sparrow, M.K. (2014). Managing the boundary between public and private policing. New Perspectives in Policing Bulletin (September 2014), Washington, DC: U.S. Department of Justice, National Institute of Justice. Retrieved from https://www.ncjrs.gov/pdffiles1/nij/247182.pdf

terminology, such as intergovernmental security management or intergovernmental security relations.[140]

There is no universal definitions that applies to all the Member States for creating and developing PPSP. In EU countries with a long tradition of strong public authority and strong public administration, there is a visible distance between public and private security sector. Public police and other security is not so eager to enter in any type of partnership with the private security sector. Even when security industry expresses the interest in creating a PPSP, the rules must be well established and goals well defined, so that the public police and other security forces know exactly what can they expect from the private security industry. There is usually a tendency to put the PPSP in a hierarchical structure reflecting the hierarchy of public administration. On the other hand, the Member States with a long tradition of sharing power between the public policing and the citizens have different approach.[141] Those EU countries usually have less hierarchical structures in public administration. The government has a very pragmatic approach to PPSP and there is no need for a legal basis – non-disclosure agreements and protocols are sufficient to set up and grow private – public security cooperation.

According to this approach, a PPSP is a contractual arrangement between a public security agency (federal, state or local) and a private security sector entity. Through this agreement, skills and assets of each sector (public and private) are shared in delivering

[140] Schaeffer, P. V., Loveridge, S. (2002). Toward an understanding of types of public-private cooperation. *Journal Public Performance & Management Review*, Vol. 26 (2), pp. 169–189

[141] Prenzler, T., Sarre, R. (2012). Public-private crime prevention partnerships. In book: Prenzler, T. *Policing and security in practice: challenges and achievements*. UK: Palgrave Macmillan, pp. 149–197

security services or facilities for the use of the general public demand of insecurity. Of course, each party of PPSP shares in the risks and rewards potential in the delivering security services.

Looking for a general PPSP definition it can be stated, that PPSP is an agreement between a public security agency and a private security sector entity that combines knowledges, skills and resources to develop a security technology, products and/or delivering security services that improves the quality of life for the general public. The private security sector has been called upon numerous times to use its resources, skills and expertise to perform specific tasks for the public security sector. Public security sector has frequently taken an active role in spurring technological advances by directly funding the private security sector to fulfil a specialized need that cannot be completed by public security sector itself.

1.2. Reasons of public-private security partnership

Nowadays in EU private security sector more and more security and policing functions, competences and assets are taken away from public security to the benefit of the private security sector. In all EU countries can be seen an increasing presence of private security companies and private security guards in the public domain. Reasons for this are numerous, for example:

1) the increasing feeling of insecurity amongst all parts of European society;
2) the limited resources of police and other public security bodies;
3) the ever-increasing quality and professionalism of private security services;

4) the innovative and flexible added value of private security sector can provide based on its longstanding expertise.[142]

The afore-mentioned reasons clearly demonstrate that well-defined, well-managed and well-monitored PPSP are efficient, effective and increase the security environment of individuals, organizations, community and states. In order to be successful, these partnerships must comply with certain criteria. These include:

1) an open dialogue between responsible public authorities and private security providers;
2) clear instructions regarding the role of each security partner;
3) a clear legal or contractual framework;
4) regular evaluation moments and necessary corrections and improvements when and where needed.[143]

In order to fulfil these criteria and to optimise the success and efficiency of PPSP and protection from security threats, risks and serious crimes (for example, terrorism, radicalism, cyber-crime), it is vital that each security partner fully understands its role, responsibilities and limits of powers. According to the CoESS' opinion that, due to a lack of specific knowledge of these elements, public–private partnerships for the security and protection of

[142] Dempsey, J. (2011). *Introduction to private security*. USA: Wadsworth

[143] Born, H., Caparini, M., Cole, E. (2007). Regulating private security in Europe: status and prospects. Geneva: Geneva Centre for the Democratic Control of Armed Forces: *Policy Paper,* No. 20. Retrieved from https://www.dcaf.ch/sites/default/files/publications/documents/PP20_Born_Caparini_Cole_.pdf

security threats and risks throughout Europe are still underdeveloped and not being used so as to reach their maximum potential.[144]

There are multiple reasons to create a PPSP.

1. Economic interests. This is the most common reason to establish a PPSP in EU. It is the usual motivation for the private security industry to participate in cooperation with the public security in the various fields of security (for example, fighting cybercrime, human trafficking and terrorism). It may establish a body which will help identifying the barriers for the growth of the security industry and create the conditions to export security products and services. Also, it could be due to a new legislation and private security industry welcoming the opportunity of influencing the process to protect its business from unnecessary or overly burdensome readjustments.
2. Regulatory requirements. PPSP model created as the implementation of a specific law whenever required and EU states governments decides that a PPSP framework will be the best way to do it. This covers mostly the case of security risk management or security law. Regulatory requirements could also include a specific law for PPSP, which provides a clear framework to the private – public security cooperation and collaboration. Mostly this type of law deals with PPSP in general. It was created to stimulate the economy, but security policy (internal and external) becoming more and more an important issue on the political agenda, PPSP are focusing on specific security threats and risks too.

[144] The new security company: integration of services and technology responding to changes in customer demand, demography and technology (5th White Paper, Berlin, 23 April 2015). Belgium: CoESS – Confederation of European Security Services, 52 p. Retrieved from http://www.coess.org/newsroom.php?page=white-papers

3. Public relations. In this case the EU states governments lets the private security sector provide input to new security legislation, as well as working together to develop a national security strategy or EU Internal Security Strategy 2015–2020.[145] For the private security sector, the motivation lies in networking with the government and other private entities (community policing) that share knowledge, skills and expertise.
4. Social interests. When the social interest was named as a driving force, it was usually the motivation to discuss security issues widely in the Member States, and set security high on the EU political agenda[146] For the private security industry, the importance lies in promoting security item in general, so that the private security market could evolve without interruption.
5. Other reasons. There are also other reasons to establish PPSP. In this category, experts explained a number of reasons, namely the new EU regulations[147], which impose new requirements on

[145] Renewed European Union Internal Security Strategy 2015–2020, approved by the European Council on 10 June 2015, No. 9798/15. Retrieved from http://data.consilium.europa.eu/doc/document/ST-9798-2015-INIT/en/pdf

[146] Shared Vision, Common Action: A Stronger Europe. Global Strategy for the European Union's foreign and security policy (2016), accepted in June 2016 by High Representative of the European Union for Foreign Affairs and Security Policy. Retrieved from http://eeas.europa.eu/archives/docs/top_stories/pdf/eugs_review_web.pdf

[147] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union. *Official Journal of the European Union*, L 194/1 (19.7.2016). Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?toc=OJ:L:2016:194:TOC&uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG;
Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). *Official Journal of the European Union*, 2016/L 119/1. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1528874672298&uri=CELEX%3A32016R0679

the private security sector. For this reason, the EU states governments may decide to create PPSP in order to help the private security industry implement the new regulations.

It should be noticed that there are often more than one reason to create a PPSP. In most cases, more than one reason needs to be met. The most common scenario is that economic and social interests exist which are accompanied by new regulation. This requires exchange of information and cooperation between private and public security entities. However, there are also a number of different motivations, which are summarized reasons to participate private and public security sectors in PPSP (Table 1).

Table 1

Reasons to participate in a PPSP

Private sector reasons to participate in a PPSP	Public sector reasons to participate in a PPSP
Access to public sector knowledge and information (EU legislation, fighting cybercrime, terrorism)	Better understanding of security industry in general
Assurance that the products delivered through PPSP are of good quality, as it is guaranteed by the government	Possibility to create synergies between different initiatives of private sector
Opportunity to influence national legislation and obligatory standards	Access to private sector resources (e.g. valuable experts), which makes it is easier to set up standards and good practices
Access to public funds	
Sharing knowledge, experiences and good practices	
Helping to achieve resilience in the security system	
Increase the trust between public-public, private-private and public–private – PPSP allows to meet different people and get to know them; because of that, it allows to have better information and proactive attitude in case of security threats, accidents and crisis	
Getting direct and credible contacts with other organisations	

Summing up, it could be seen that the cultural dimension of European countries is one of the most important determinants of establishing, developing and functioning PPSP. Due to cultural differences, there is no universal scenario on how to create a successful PPSP. PPSP model followed in one country will not necessarily fit another.

1.3. Privatization of security services as outcome of public-private security partnership

Tendencies of *privatisation of security services* is a new social phenomenon, which influences Member States legal system and gives rise to academic and practical debate.[148]

Concept *"privatization of security services"* (Anglo–Saxon researchers used the term *"privatization of policing"*[149] range from a general shrinking of the state to the more precise replacement of public security bodies with private security sector entities. Private security sector leading the privatization process, where it is spontaneously developing alongside with *community policing* model.[150] The message sent here is that in a free movement market and democratic society private resources may be employed in

[148] Kalesnykas, R. (2007). Privatization processes of policing in Lithuania. *SIAK Journal: Zeitschrift für Polizeiwissenschaft und Polizeiliche Praxis*. Wien: Bundesministerium für Inneres, No. 3, pp. 14–24

[149] Prenzler, T., Sarre, R. (2012). Public-private crime prevention partnerships. In book: Prenzler, T. *Policing and security in practice: challenges and achievements*. UK: Palgrave Macmillan, pp. 149–197;

Sarre, R, Van Steden, R. (2011). The growth of privatized policing: some cross-national data and comparisons. *International journal of comparative and applied criminal justice*, Vol. 31 (1), pp. 51–71

[150] Miller, L. S., Hess K. M., Christine H. (2017). *Community Policing: partnerships for problem solving*. USA, Boston: Cengage Learning

public or national security area, whereas the efficiency largely depends on the competitive market of security services providers as a whole. The ultimate efficiency of the implementing security function may be achieved when powers and competences of the two security services providers (public and private sector) are properly balanced.

Privatization of security services occurs typically on both the revenue-raising side and on the spending-and-production side.[151] On the revenue-raising side, citizens or organizations allocate the funds for security services that might otherwise be provided publicly and determine how they will be allocated, for example hiring of private security guards and private investigators, installation of CCTV, lighting and alarm systems, patrolling or escort services and so on. On spending-and-production side, state or local governments may contract with private security companies for such specific services as court security, prisoner custody, IT and communications system maintenance, traffic and parking control and so on.

PPSP as the outcome of privatization has advanced considerably over the last decade. The UN Office of Drugs and Crime has made efforts to promote PPSP, stating that "private security needs to be considered in national and local government plans and partnership consultation for a number of reasons, but especially to ensure the inclusiveness of prevention strategies and the equality of security provision"[152]. Public and private security institutions cooperate in a number of areas, including responding to crimes, crime prevention

[151] Kalesnykas, R. (2001). Certain problems of privatization of the police functions in Lithuania. *Jurisprudence: academic journal of Mykolas Romeris University*, Vol. 19 (11), pp. 190–201

[152] Handbook on the crime prevention guidelines: Making them work (2010). Vienna: UN Office on Drugs and Crime. Retrieved from http://www.unodc.org/documents/justice-and-prison-reform/crimeprevention/10-52410_Guidelines_eBook.pdf

and investigating crime, sharing intelligence and knowledge. Private security can augment public police in a "value added", "extra eyes and ears" role, or may assume a primary role, including being hired to patrol neighbourhoods.[153] Today, the requirements for effective PPSP include:

1) a tangible purpose;
2) common tasks;
3) the specificity of the mission, (i.e. to address specific problems of security);
4) knowledge of the capabilities;
5) agreement as to how the partnership will function;
6) the type and level of funding;
7) leadership (with some led by the police, others by private security, and still others have a joint leadership arrangement);
8) inclusiveness, wherein some partnerships include a number of police services and businesses, while others are more limited in the scope of the partnership;
9) a mutual commitment to provide the resources required to sustain the partnership.[154]

Concluding above-mentioned proposition, we could considered that *privatisation of security services* is treated as a process of transference of certain obligations of public policing as well as responsibilities from public security bodies to private security entities. In such context, PPSP have been integral to the advancement of security science and technology for the common good through

[153] Mulone, M. (2012). When Private and Public Policing Merge: Thoughts on Commercial Policing. *Social Justice*, Vol. 38 (1–2), pp. 65–83

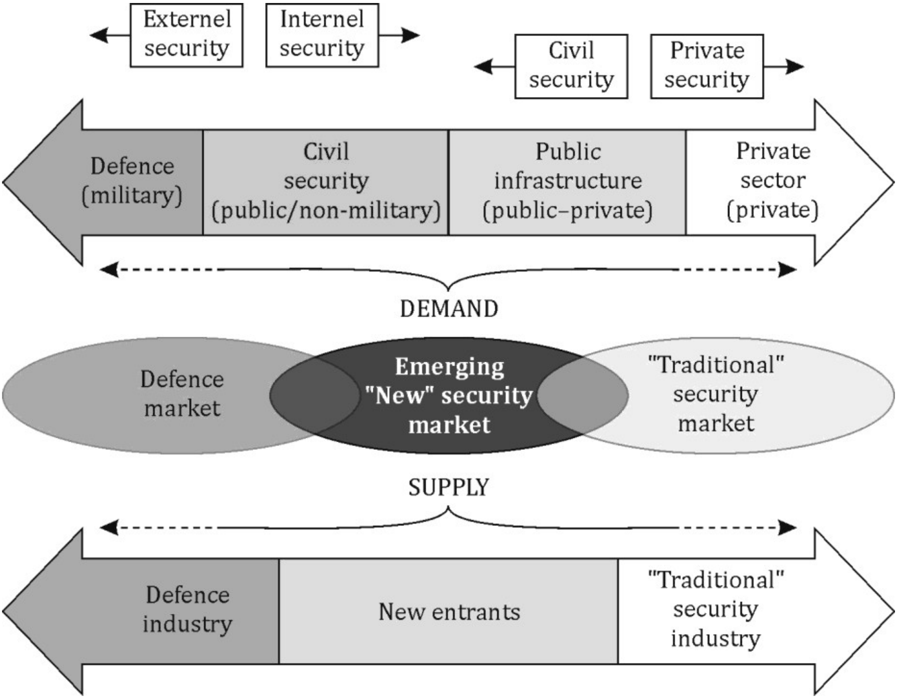
[154] Morabito, A., Greenberg, S. (2005). *Engaging the private sector to promote homeland security: law enforcement – private security partnerships*. Washington, D.C.: Bureau of Justice Assistance

the efficient completion of tasks and requirements, a decrease in the amount of taxpayer money spent, improvement of government compliance with the living environment and the enhancement of the quality of security products and services. Partnership agreements between public and private security sector entities have involved the public security sector funding to the private sector to divert its time and resources to address an area without the potential of acceptable return on investment.

3. Security market development in the European Union

Security industry is neither well defined nor clearly identifiable. In fact, the production and supply of security-related equipment and systems, services and applications, may be found under a wide range of industry and services headings that cover both non-security and security-related activities. Taking into consideration the nature of security threats and risks, priorities, demand and supply-side characteristics, Figure 1 provides a general overview of the security market.

Figure 1 (p. 192) shows that there is a general distinction between two different security threat categories: "Traditional security", corresponding to protection against threats such as "ordinary" criminal activity, fire protection, etc., and "New security", corresponding to protection against threats such as terrorism, organised crime, cyber-crime, etc. In terms of a general categorisation of demand-side security, two distinctions are made: *first,* between "external" and "internal" security dimensions and, secondly, between "public" and "private" security responsibilities. It is useful to note that the boundaries between the different segments identified above are often not clearly defined. From a demand perspective, there


Externel security
Internel security
Civil security
Private security
Defence (military)
Civil security (public/non-military)
Public infrastructure (public–private)
Private sector (private)
DEMAND
Defence market
Emerging "New" security market
"Traditional" security market
SUPPLY
Defence industry
New entrants
"Traditional" security industry

** Source Ecorys (2015)*

Figure 1. **Architecture of the security market**

can often be an overlap in terms of the allocation of security responsibilities and the role of different demanders of security products or services. On the supply side, the acquisition of primarily civilian technology suppliers by defence industry companies thus blurring the distinction between defence and security. At the same time, “new” security threats have both raised demand for traditional security products and led them to acquire or develop new technologies, such that a clear separation cannot be made between the “traditional” security industry and a “new” security industry.[155]

Private security has become a major contributor to overall security policy in EU. Provision of security services is common to all, the public and private security industries differ in terms of structure, command, aims and methods. Private security sector comprises a large range of activities, including surveillance of personal assets and property, cash-in-transit, personal protection, access control and designing, installing and alarm systems management. Private security industry is neither homogenous nor structured.

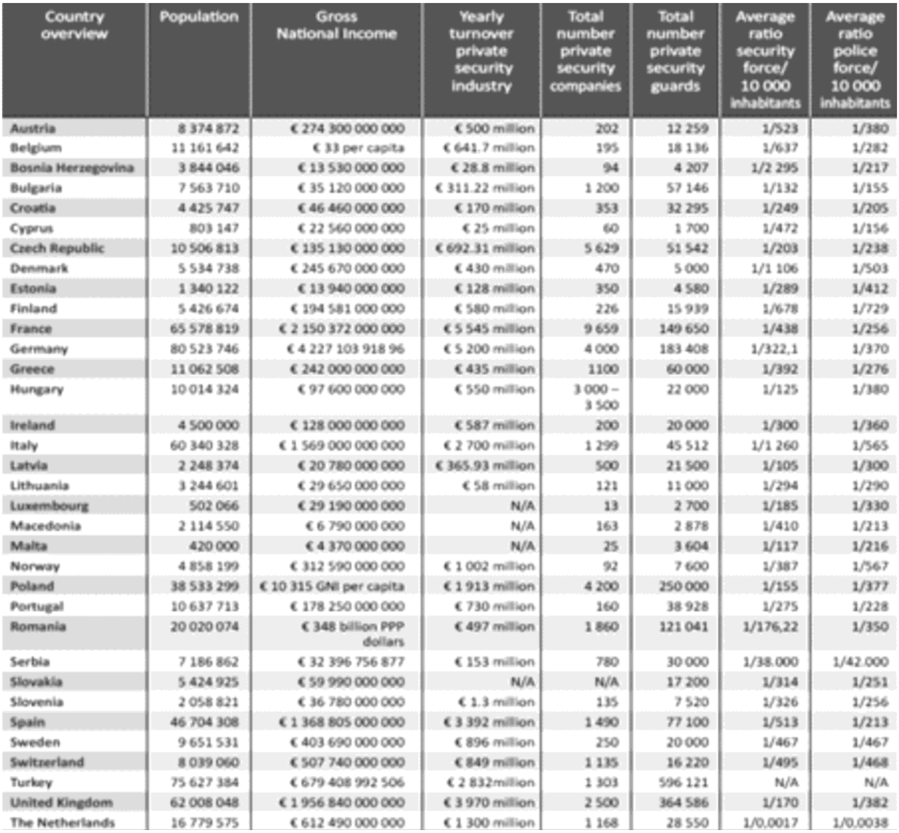
Presenting a European quantitative overview of the private security industry is unique, since scientific research on the matter is scarce. CoESS is the European umbrella organisation for 25 national private security employers’ associations and has a tradition in presenting a quantitative overview of European security services, called “Facts and Figures”.[156] Today private security industry is one of the fastest growing business sector in Europe and this can be seen from the gross national income, yearly turnover from the private security industry, the total number of private security companies, average ratio security force per 10 000 inhabitants and the average ratio police force per 10 000 inhabitants (Table 2).

[155] Study on the development of statistical data on the European security technological and industrial base (June 2015). The Netherlands, Rotterdam: ECORYS. Retrieved from https://ec.europa.eu/home-affairs/sites/homeaffairs/files/e-library/documents/policies/security/reference-documents/docs/security_statistics_-_final_report_en.pdf

[156] The new security company: integration of services and technology responding to changes in customer demand, demography and technology (Fifth White Paper, Berlin, 23 April 2015). Belgium: CoESS – Confederation of European Security Services, 52 p. Retrieved from http://www.coess.org/newsroom.php?page=white-papers

Table 2

Private security industry in Europe



Country overview	Population	Gross National Income	Yearly turnover private security industry	Total number private security companies	Total number private security guards	Average ratio security force/ 10 000 inhabitants	Average ratio police force/ 10 000 inhabitants
Austria	8 374 872	€ 274 300 000 000	€ 500 million	202	12 259	1/523	1/380
Belgium	11 161 642	€ 33 per capita	€ 641.7 million	195	18 136	1/637	1/282
Bosnia Herzegovina	3 844 046	€ 13 530 000 000	€ 28.8 million	94	4 207	1/2 295	1/217
Bulgaria	7 563 710	€ 35 120 000 000	€ 311.22 million	1 200	57 146	1/132	1/155
Croatia	4 425 747	€ 46 460 000 000	€ 170 million	353	32 295	1/249	1/205
Cyprus	803 147	€ 22 560 000 000	€ 25 million	60	1 700	1/472	1/156
Czech Republic	10 506 813	€ 135 130 000 000	€ 692.31 million	5 629	51 542	1/203	1/238
Denmark	5 534 738	€ 245 670 000 000	€ 430 million	470	5 000	1/1 106	1/503
Estonia	1 340 122	€ 13 940 000 000	€ 128 million	350	4 580	1/289	1/412
Finland	5 426 674	€ 194 581 000 000	€ 580 million	226	15 939	1/678	1/729
France	65 578 819	€ 2 150 372 000 000	€ 5 545 million	9 659	149 650	1/438	1/256
Germany	80 523 746	€ 4 227 103 918 96	€ 5 200 million	4 000	183 408	1/322,1	1/370
Greece	11 062 508	€ 242 000 000 000	€ 435 million	1100	60 000	1/392	1/276
Hungary	10 014 324	€ 97 600 000 000	€ 550 million	3 000 – 3 500	22 000	1/125	1/380
Ireland	4 500 000	€ 128 000 000 000	€ 587 million	200	20 000	1/300	1/360
Italy	60 340 328	€ 1 569 000 000 000	€ 2 700 million	1 299	45 512	1/1 260	1/565
Latvia	2 248 374	€ 20 780 000 000	€ 365.93 million	500	21 500	1/105	1/300
Lithuania	3 244 601	€ 29 650 000 000	€ 58 million	121	11 000	1/294	1/290
Luxembourg	502 066	€ 29 190 000 000	N/A	13	2 700	1/185	1/330
Macedonia	2 114 550	€ 6 790 000 000	N/A	163	2 878	1/410	1/213
Malta	420 000	€ 4 370 000 000	N/A	25	3 604	1/117	1/216
Norway	4 858 199	€ 312 590 000 000	€ 1 002 million	92	7 600	1/387	1/567
Poland	38 533 299	€ 10 315 GNI per capita	€ 1 913 million	4 200	250 000	1/155	1/377
Portugal	10 637 713	€ 178 250 000 000	€ 730 million	160	38 928	1/275	1/228
Romania	20 020 074	€ 348 billion PPP dollars	€ 497 million	1 860	121 041	1/176,22	1/350
Serbia	7 186 862	€ 32 396 756 877	€ 153 million	780	30 000	1/38.000	1/42.000
Slovakia	5 424 925	€ 59 990 000 000	N/A	N/A	17 200	1/314	1/251
Slovenia	2 058 821	€ 36 780 000 000	€ 1.3 million	135	7 520	1/326	1/256
Spain	46 704 308	€ 1 368 805 000 000	€ 3 392 million	1 490	77 100	1/513	1/213
Sweden	9 651 531	€ 403 690 000 000	€ 896 million	250	20 000	1/467	1/467
Switzerland	8 039 060	€ 507 740 000 000	€ 849 million	1 135	16 220	1/495	1/468
Turkey	75 627 384	€ 679 408 992 506	€ 2 832million	1 303	596 121	N/A	N/A
United Kingdom	62 008 048	€ 1 956 840 000 000	€ 3 970 million	2 500	364 586	1/170	1/382
The Netherlands	16 779 575	€ 612 490 000 000	€ 1 300 million	1 168	28 550	1/0,0017	1/0,0038

** Source CoESS (2013)*

There were 44.811 enterprises operating within the private security and investigation services sector in the EU-28 in 2015. They employed 1.94 million persons, which was equivalent to 1.5 % of the total workforce within the non-financial business economy. EU-28 security and investigation services enterprises generated EUR 39.7 billion of value added which was equivalent to 1.1 % of the non-financial business economy total or 8.5 % of the administrative and support services total.[157]

Almost 7 in every 10 private security companies within the EU-28's security and investigation services sector were classified as operating within the private security activities subsector, while just under one in five operated within the security systems service activities subsector, leaving the residual (one in ten) engaged in investigation activities (Figure 2). Respectively, almost 90 % of the total employment is reflected under security sector implementing general private security functions.

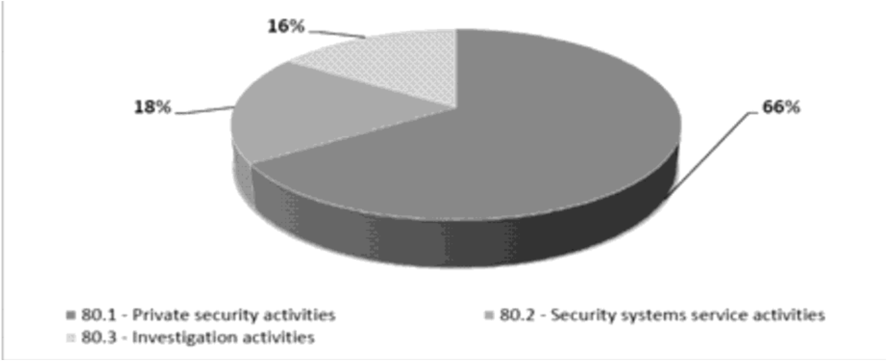


Figure 2. **Fields of activities of private security companies (%)**[158]

According to the CoESS[159] presented results, the average age of a private security guard working in the EU private security industry

[157] The new security company: integration of services and technology responding to changes in customer demand, demography and technology (Fifth White Paper, Berlin, 23 April 2015). Belgium: CoESS – Confederation of European Security Services, 52 p. Retrieved from http://www.coess.org/newsroom.php?page=white-papers

[158] Ibid

[159] Ibid

is 36 years old and the average percentage of men active in the private security industry is ±83 % versus ±17 % for women. Regarding the power and competences of private security guards, we can indicate that in ±59 % of all the EU countries private security guards have the same rights as any other citizen. In ±61 % of EU countries, private security guards are allowed to perform a search and seizure (full or limited).

The use of weapons is allowed in ±82 % of the EU countries and in ±82 % of the cases a special licence is required for private security companies providing armed private security services. Private security guards must follow specialised and obligatory training (by law) in order to be able to carry and use weapons in all of the Member States. A special license is required for private security companies using dogs for the provision of private security services (±44 % of all the EU countries) and private security guards must follow a specialised and obligatory training (by law) in order to be able to use dogs for the provision of private security services (57 % of all the EU countries).

Private security industry clearly defined market segments as providing basic security services (physical, commercial and in-house manned), bodyguarding, ascertaining material facts, fire prevention and protecting services, safety of track construction, mobile alarm response and call-out services, cash-in-transit services and transporting valuables, CCTV monitoring and installation, security manager, loss prevention, private investigation and security consulting, aviation security, urban security – train/metro stations, city patrols, maritime security, critical infrastructure protection and guarding military units). In addition, a number of security market segments are being developed, for instance, penitentiary system management, critical infrastructures, community guards, which in turn can make use of the effects of the already acquired efficiency and effectiveness of existing security market segments.[160]

As seen on EU population changing demands for security, the private security industry continues to grow and become more and more adaptable, offering a broad spectrum of security services. This may impact on the state and civil society's ability to hold the private security industry accountable, as security services are becoming increasingly interdependent with public resources.[161] The socio-economic added value provided by the private security companies consists of the improved or additional value for EU security so that the total value of security increases for and as a result of public authorities, the business community and the citizen. Private security services represent an additional complementary partner in total security (risk) management system.

3. Regulatory framework for security partnership

An important point to be taken into account with regard to a PPSP is that of the public and private laws both at a national (Member State) level and at a European level should be harmonized and the existence of such type of security partnership model should be legitimized. In fact, the analysis of the current regulatory framework of PPSP shows that still no harmonisation of legislation concerning the private security industry at the European level has yet taken place. The CoESS promote minimum requirements for private security companies at the European level, for example, in

[160] Critical infrastructure security and protection: the public-private opportunity (2016). Belgium: CoESS – Confederation of European Security Services, p. 98. Retrieved from http://www.coess.org/newsroom.php?page=white-papers

[161] Berg, J. (2007). The accountability of South Africa's private security industry: mechanisms of control and challenges to effective oversight. Newlands, South Africa: Criminal Justice Initiative of the Open Society Foundation for South Africa.

the area of licensing, vocational training or entrance requirement for private security personnel.[162] Nevertheless, at present national regulations of private security industry differ from one Member State to another and reflect the different cultural environments. Some areas of the private security industry are more regulated than others. For instance, the providers of airport security fall under the EC regulation establishing common rules in the field of civil aviation security, which therefore contains some rules that directly affect private security personnel. Indeed, the regulation states that all staff requiring access to security-restricted areas will be subjected to a minimum 5-year background check, and will also receive regular training in aviation security.[163]

Another interesting point of view is that private security companies were excluded from the EU Directive for services in internal market.[164] CoESS argued that the specific nature of private security entities, in particular its close links to the issue of public security, and the necessity for strict conditions for entering the security market necessitates specific exceptions that could not be sufficiently taken into account in the general directive.[165] CoESS has

[162] Private Security services in Europe: CoESS Facts and Figures 2013. Belgium: CoESS – Confederation of European Security Services. Retrieved from http://www.coess.org/newsroom.php?page=facts-and-figures

[163] Regulation (EC) No 300/2008 of the European Parliament and of the Council of 11 March 2008 establishing common rules in the field of civil aviation security and repealing Regulation (EC) No 2320/2002. Official Journal of the European Union, 2008/L 97/72. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32008R0300

[164] Directive 2006/123/EC of the European Parliament and of the Council of 12 December 2006 on services in the internal market. *Official Journal of the European Union*, 2006/L 376/36. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32006L0123

[165] Private security and its role in European security (Fifth White Paper, Paris, December 2008). Belgium: CoESS – Confederation of European Security Services, 98 p. Retrieved from http://www.coess.org/newsroom.php?page=white-papers

highlighted the fact that an overview of Member States demonstrated that the level of effective security is positively correlated to the level of regulation in the private security industry.[166] This underlines the importance of achieving a harmonisation of the regulation and the need for high standards on private security companies at the European level. Argument for such approach is that PPSP legislation is necessary to make private security companies accountable for their actions. Particularly since a major difference between private security companies and state public security providers is that the latter are directly accountable to parliament, government and the public, whilst private security companies only have to respond to shareholders and clients.

Indeed, regulation of PPSP can be interpreted as the usually formal mechanisms of risk management and control, which are established in order to guide conduct of each security partner and to ensure the universal application of the law. In terms of the PPSP model, the EU acknowledges that private security companies constitute an important part of each Member State's security system.

4.1. Legal regulation of public-private security partnership

The regulation of private security industry is meant as a state intervention in private spheres of activity to realize public purposes.[167] The private security industry is subject to great deal of regulation relating to EU and international law, security law,

[166] The new security company: integration of services and technology responding to changes in customer demand, demography and technology (Fifth White Paper, Berlin, 23 April 2015). Belgium: CoESS – Confederation of European Security Services, 52 p. Retrieved from http://www.coess.org/newsroom.php?page=white-papers

[167] Sarre, R. (2004). The future of policing in a broader regulatory framework. In Johnston R. and Sarre R. (eds). *Regulation: Enforcement and Compliance*. Australian Institute of criminology

administrative law, company law, employment law and health and safety legislation and so on. Current legislation on private security industry in some Members States abounds in some loopholes and discrepancies not only in terms of interpretation but also in terms of its application. At this juncture, the role of private security entities in the participation or realization of PPSP model is eclectic due to the vague description of their functions and competences. Setting of efficient legal standards has become a topical issue for the subjects in question as they seek to ensure professional and top quality security services. Social norms and legal acts would *first*, facilitate activities of private security, *second*, protect from negative tendencies or from what is unacceptable for private security.

In Member States, the private security companies are regulated solely on a national basis. The main goal of these regulations is to protect citizens from the misuse of power, to promote transparency and to deter the creation of paramilitary groups.[168] National regulation is used as the necessary tool to guarantee the quality of the services offered and protect against human rights violations. In that matter each national regulatory system succeeds in the stabilisation of the private security market while improving the professionalism of the security industry and strengthening the profession of security staff.

In a research study published by CoESS in 2013, rigid examples of the different levels of regulation of private security companies could be observed.[169] In this research the national differentiation of legal regulation of private security companies in

[168] Cvrtila, V., Perešin, A. (2014). New security models and public-private partnership. *Collegium antropologicum*, Vol. 38, No. 1, pp. 195–204

[169] Private Security services in Europe: CoESS Facts and Figures 2013. Belgium: CoESS – Confederation of European Security Services. Retrieved from http://www.coess.org/newsroom.php?page=facts-and-figures

the EU countries was indicated. CoESS experts' presents EU legislative mapping based on criteria of strictness of national-level private security legislation across Europe: very strict, strict, medium, low (Table 3).

Table 3

Strictness of private security legislation at national level in EU countries[170]

Low	Medium	Strict	Very strict
Austria Czech Republic Poland	Ireland United Kingdom France Germany Bulgaria Latvia Cyprus	Greece Romania Croatia Slovenia Slovakia Italy Switzerland The Netherlands Estonia Lithuania Denmark Finland Malta	Hungary Belgium Sweden Portugal Spain Luxembourg

CoESS experts[171] outlined the main regulatory systems that exist in the EU private security market.

1. Member States with flexible legislative provision of private security sector (Poland, Germany, the Czech Republic, Austria, Cyprus).

[170] Private Security services in Europe: CoESS Facts and Figures 2013. Belgium: CoESS – Confederation of European Security Services. Retrieved from http://www.coess.org/newsroom.php?page=facts-and-figures

[171] Private security and its role in European security (Fifth White Paper, Paris, December 2008). Belgium: CoESS – Confederation of European Security Services, 98 p. Retrieved from http://www.coess.org/newsroom.php?page=white-papers

There is no specific legislation regulating private security industry. Here, various provisions from civil, commercial or penal legislation apply. Private security companies extra powers – such as the use of weapons – are regulated by general gun laws that apply to every citizen in the jurisdiction.

2. Intermediate (or mixed) legislative provision of private security sector. In such Member States (France, Slovenia, Slovakia, Italy, Denmark, etc.), private security companies are seen as economic operators who provide services that resemble the exercise of public power. More over their extra powers are regulated sectorally and in some cases, requirements for training and approving agents and entrance restrictions are set out.
3. Strict systems in the regulation of private security sector. In such EU countries (Belgium, Sweden, Portugal, Spain), the specialized laws (known as the private security and particular security act) defines the criteria covering uniforms, equipment, weapons, vehicles, watchdogs, training and private security conditions on companies' financial resources. Police-like functions of private security companies are addressed and regulated in order to protect citizens and enhance the operation of the private security industry.[172]

According to the national laws of Members States, private security companies usually cannot provide services and activities that are/would normally be reserved to police forces or other public security authorities (Ireland, Malta, Poland, Romania, Slovenia, Slovakia). But there are number of EU countries in which private

[172] Private security and its role in European security (Fifth White Paper, Paris, December 2008). Belgium: CoESS – Confederation of European Security Services, p. 98. Retrieved from http://www.coess.org/newsroom.php?page=white-papers

security companies can provide services and activities that are/would normally be reserved to police forces or other public security authorities. For instance, in Belgium private security companies are supporting police forces, making statements regarding the immediately observable situation of goods on the public domain and guaranteeing road safety; in Lithuania and Estonia handling of speed cameras or ensuring public order during mass events; in Finland private security companies assist the police in investigations, keeping the public order and security in listed public places; in Spain and Portugal private security companies provided services in prisons, foreign detention centres, public premises and participate in provision of services mandated to public security. There is an increasing trend of transferring police competences (totally or in support) towards private security companies in some EU countries, for example, in Croatia, Germany, the Netherlands – airport security, in Greece – guarding services in embassies and athletic events, in Luxembourg, Lithuania, Latvia, Estonia – delegation of activities which do not belong to the core competences of police services, such as parking control and railway security, in UK – prisoner transport, prison services and migration services too.

Currently there is discussion on desirability of regulating the private security industry in the Member States and setting the minimum standards to private security companies. Such regulatory requirements may include the following:

1) roles and competence of private security companies;
2) links between private security companies and public police/public security agencies;
3) control and accountability of private security companies;
4) entrance requirements of private security personnel;
5) selection and recruitment of private security personnel;
6) training of private security personnel;

7) identification of private security personnel;
8) use of firearms by private security personnel;
9) search and seizure powers of private security companies.

It is assumed that one of the most important issues in the legislative process of private security industry involvement in PPSP is the settlement of clear competences. The following private security competences can be distinguished in the area of PPSP:

1) crime prevention. This group of private security companies activities includes patrolling, guarding of private property, guarding of (nuclear) power plants, installations of CCTV, airport and maritime security; detention of intrusion, unaut-horized entry, vandalism or trespassing on private property;
2) detection of theft, loss, embezzlement, misappropriation or concealment of merchandise, money, bonds, stocks, notes, valuable documents or papers, for example, protection of cash in transit;
3) protection of individuals from bodily harm, e.g. bodyguards;
4) enforcement of established company rules, regulations, measures, policies and practices related to crime reduction;
5) maintaining public order at events (concerts, football matches);
6) reporting and apprehension of violators;
7) transporting prisoners and guarding prisons;
8) reporting on and responding to incidents and calls, including the conception, installation and maintenance of alarm systems and alarm centres.[173]

[173] Born, H., Caparini, M., Cole, E. (2007). Regulating private security in Europe: status and prospects. Geneva: Geneva Centre for the Democratic Control of Armed Forces: Policy Paper No. 20. Retrieved from https://www.dcaf.ch/sites/default/files/publications/documents/PP20_Born_Caparini_Cole_.pdf

Summing up we could believe that in the future private security companies will be one of the most important players in the field of PPSP. Of course, EU and Member States should solve all regulatory issues and set up legal standards of implementing PPSP. EU must adequately plan and manage the PPSP process with due regard to the current situation in security industry. In order to achieve this it is necessary to establish the clear vision and role of the each Member State in the process. Existing differences in regulation of private security industry make it impossible to proceed with a clear-cut categorization of the regulatory systems in EU countries.

4.2. Accountability issue in public-private security partnership

Today the role and mission of private security industry is not rightly defined in many Member States and the relevant legal mechanism still does not work smoothly. Knowledge based community and e-society domination lets us to understand the cooperation between public and private security in a broader sense and relates it to ensuring of control in all spheres of social life, so that human rights and freedoms are protected, safety needs of society, organization and individuals are met and laws are abided.

PPSP is a cooperation agreement between autonomous private and public security entities working together to achieve joint purposes, based on a clear division of responsibilities, tasks and authority, and with no hierarchy amongst the parties. The most important preconditions for the success of a PPSP are mutual trust and recognition of the possibilities for the future. Most PPSP model participants as being the responsibility of the organisations security concerned see the accountability of private security sector. Should this be lacking, the Member States governments should assume its responsibility by investigating and prosecuting and where necessary, altering legislation.

An approach to the issue of public and private security accountability largely stems from an understanding of how the private and public security interact and relate to each other and what similarities and differences they have to each other.[174] If we contend that the private security industry is more similar to the state police, we will most likely adopt a means of holding the private security industry accountable taking into account its relation to other bodies rather than attempting to hold it accountable in isolation. To assess the effectiveness of the oversight mechanisms we can take Dixon's four-dimensional view of accountability, which can be applied to 'any organisation involved in security'. According to this view, accountability involves content, direction, mode and mechanism.[175] Focusing on legislating of private security entities, the state should also consider how it can facilitate the development of partnerships between public security entities to enable them to work together more effectively. For this reason, discussions on accountability in PPSP become extremely complex.

The content of accountability in PPSP means the types of activity that the public and private security entities need to be held accountable for. Research studies identified different types of the accountability of PPSP:

1) internal accountability (how the industry can hold itself accountable, i.e. marketplace accountability, self-regulation, code of conduct);
2) accountability through the state (how the state has promoted accountability, i.e. legislation, audit and control,

[174] Berg, J. (2007). The accountability of South Africa's private security industry: mechanisms of control and challenges to effective oversight. Newlands, South Africa: Criminal Justice Initiative of the Open Society Foundation for South Africa

[175] Dixon, B. (2000). Accountable Policing: A Four Dimensional Analysis. *South African Journal of Criminal Justice*, No. 13(1), pp. 69–82

personnel training standards, special commissions, rights of the security employees);

3) accountability through civil society (social control mechanisms holding the partnership accountable, i.e. media interpretations, non-governmental organisations, human rights monitoring organisations.[176]

Most Member States national regulation makes very clear distinctions between the private security industry and public security sector entities. In terms of private security entities similarity to the state police and the oversight challenges that PPSP creates, legislation prompts both a proactive and reactive regulation of private security industry in conjunction with the other types of accountability mechanism. In this case, there is another trend of security tradition among each member States and in the people's beliefs and attitudes toward the partnership between the private and public sector in the field security. Many EU countries are facing the PPSP model of guaranteeing security in general that brings harmonization of law, managing risks, development of code of ethics and standardization the security services.

4.3. Risks of public-private security partnership

As can be seen from the above provided data, the growth and size of private security market has led to calls for a greater co-operation with police and for formal PPSP. However, there are numerous risks to a closer working relationship. In the first instance, the two groups operate on fundamentally opposing principles. Police

[176] Kalesnykas, R. (2012). Accountability and integrity issues in public-private security cooperation. In book "Policing and Security: CEPS 2012", 4–5 October 2012. Melbourne, Australia: Centre of Excellence in Policing and Security, pp. 23–28

have a duty to serve the public equally on the basis of need, whereas private security providers are, for the most part, obliged only to their employer or principal.[177] Furthermore, forms of cooperation between police and private security firms could potentially involve a skewing of public resources towards the firms and their customers. There have also been significant cultural differences between police and private security.[178] Police have generally looked down on private security guards and investigators as less professional. Despite some high skill levels in private security, this situation derives in part from the lower training, selection and salary standards that generally apply to private security officers.

There are four types of reasons to the risks in PPSP:

1) reasons, which hinder start-up and maintenance of close relations between the public and private security entities in carrying out common functions of public safety and public order, i.e. afraid of competition, which is one of the negative presumptions to carry out common activities;
2) reasons, which stimulate partnership between the police and private security entities, i.e. fixing of legal, contractual and administrative relations which take shape in maintenance of common functions for ensuring the protection of personal, organization, public or state safety;
3) private security – contract-based activity, i.e. the main focus driven to private but not to public interest. Usually this discrepancy is called conflict – based security;

[177] Prenzler, T., Sarre, R. (2012). Public-private crime prevention partnerships. In book: Prenzler, T. *Policing and security in practice: challenges and achievements*. UK: Palgrave Macmillan, pp. 149–197

[178] Kalesnykas, R. (2002). Possibilities to integrate the private security in the system of law and order. *Jurisprudence: Academic Journal of Mykolas Romeris University*, No. 26 (18), pp. 71–82

4) control of private security activities by the public police, i.e. there still exists mistrust to the private security, requirement to the license for activity, public police and private security operate in distinct areas and response to different interest and so on.

Accordingly, these risks resulted challenges in implementing PPSP model, for example, lack of human resources in both the public and private security sector, insufficient public security sector budget and resources fail to meet the private security sector's expectation, establishment of a common level of understanding and dialogue between the public and private security sector, lack of leadership and legal basis, promotion of the concept of PPSP. In order to properly manage risks and challenges faced to realization PPSP, the following actions may be taken:

1) motivation for the private security sector to participate should be a priority when establishing a PPSP. To create successful and efficient PPSP, resources are needed. PPSP will not grow if there is a lack of people who will work on them. PPSP need a whole group of people who prepare the action plans and work closely with both public security bodies and private security sector entities;
2) participants should agree on creating a legal base for PPSP. If no legal framework for the cooperation, the whole process of creating and developing a PPSP will be slow and not efficient;
3) legal basis could be a national legal act or a memorandum of understanding (MoU), which apply to everyone and every member should know what kind of input they should provide and what kind of benefits they may expect from PPSP;

4) government should lead the PPSP. Private security sector expects government to act. If the public security sector could agree for the one contact point for PPSP, that could be enormously beneficial for the overall PPSP. Since security is highly interdisciplinary, there are usually many public bodies involved in PPSP – Ministry of Internal Affairs, Ministry of Defence, Ministry of Economy. It is very important that government entities involved in a PPSP should know in advance, i.e. before inviting private security sector partners to join – what they want to achieve, what their contribution is going to entail, and what the private security sector should contribute;
5) public and private security sector participants should invest in open communication and a pragmatic approach towards building a PPSP. If the members of PPSP do not communicate in an honest and open way, they can be victims of their expectations, which neither private nor public security sector will be able to meet.

Consequently, in many European countries still dominates an opinion that the public police and other public security bodies still remain the most important public security organizations in the multiplicity of agencies involved in security. Contrary to popular belief, due to limited resources today sees the incapacity of the state to guarantee proper level of security and maintain public order, which is in particular true in relation to the protection of private business. The integrity issues in PPSP reveal the vast diversity of state's security culture in Europe. All models co-exist, from established monopolies to shared responsibilities, with federal, regional, national or mixed security styles clearly prevailing.

Conclusions and recommendations

1. The domination of PPSP phenomena in a security area depends on economic, social, political, risk management and legal conditions in EU and each Member States. Such phenomena allow narrowing and purging the functions of public police and other security agencies and extending the range of security services provided by private security companies. Provision of public and private partnership in security industry/market may also be a business, the distinguishable feature of which is that efficiency of the security services depends on competition between public and private security institutions.
2. Member States has various regulatory mechanisms of private security industry. They describe the legal status of private security companies superficially and does not protect from negative trends in private security market. Relationship between the public and private security sector are still complicated. The fact is that the public police are typically regulators of private security companies as well as potential competitors in the provision of security services. However, in many circumstances police and private security institutions have quite different powers, competences and responsibilities. Despite different operating principles, it does appear to be possible to develop PPSP that address security threats and insecurity problems in ways that benefit a variety of stakeholders, including the general public and taxpayers.
3. The range and scope of private security services indicates that private security sector is becoming an alternative to public police services. Narrowing functions of the public security institutions and widening the range of security services provided

by private security companies allows thinking of abrogation of monopoly in security industry. This situation makes it possible to think of removal of the state monopoly in the many spheres of providing security services.

4. Research studies highlighted synergy of public and the private security sectors. Society requires the clear and transparent security services, accountability and responsibility of each public and private security sector partner. Public trust is an essential prerequisite for effective security services provision, whether such provision is by the public police, private security, or by both in partnership with each other. In PPSP model, private security sector is better positioned to align their knowledge, expertise and technology offerings to needed capabilities within the state and its stakeholders.
5. EU and each Member States government should provide full support for the development of private security market. However, it is very important to evaluate private security companies possible input in the protecting of persons and property, enforcement security in public places and participating in crime prevention. Well-regulated private security market could guarantee high quality of security services and these services may be implemented in the most effective way.
6. In the future, it is recommended for EU to create a common regulatory PPSP model for all Member States, which will harmonize legal differences of private security market between Member States, re-evaluate and redefine contemporary public–private security sector collaboration strategies, contextualize the precise nature and role of private security companies, set high-level standards for private security service providers within the EU (including appropriate levels of security screening

of staff and equitable remuneration), ensure reporting of private security companies' irregularities and illegalities and make it possible to hold them accountable for legal violations, including human rights violations.

References

Berg, J. (2007). The accountability of South Africa's private security industry: mechanisms of control and challenges to effective oversight. Newlands, South Africa: Criminal Justice Initiative of the Open Society Foundation for South Africa

Born, H., Caparini, M., Cole, E. (2007). Regulating private security in Europe: status and prospects. Geneva: Geneva Centre for the Democratic Control of Armed Forces: *Policy Paper*, No. 20. Retrieved from https://www.dcaf.ch/sites/default/files/publications/documents/PP20_Born_Caparini_Cole_.pdf

Brogden, M., Nijhar, P. (2013). *Community Policing*. UK, London: Routledge

Button, M. (2002). *Private Policing*. UK: Willan Publishing

Critical infrastructure security and protection: the public-private opportunity (2016). Belgium: CoESS – Confederation of European Security Services, p. 98. Retrieved from http://www.coess.org/newsroom.php?page=white-papers

Cvrtila, V., Perešin, A. (2014). New security models and public-private partnership. *Collegium antropologicum*, Vol. 38, No.1, pp. 195–204

Dempsey, J. (2011). *Introduction to private security*. USA: Wadsworth

Dixon, B. (2000). Accountable Policing: A Four Dimensional Analysis. *South African Journal of Criminal Justice*, No. 13(1), pp. 69–82

George, B., Button, M. (2000). *Private Security*. UK, Leicester: Palgrave Macmillan

Handbook on the crime prevention guidelines: Making them work (2010). Vienna: UN Office on Drugs and Crime. Retrieved from http://www.unodc.org/documents/justice-and-prison-reform/crimeprevention/10-52410_Guidelines_eBook.pdf

Johnston, L. (2005). *The Rebirth of Private Policing*. London: Routledge

Kalesnykas, R. (2001). Certain problems of privatization of the police functions in Lithuania. *Jurisprudence: academic journal of Mykolas Romeris University*, Vol. 19 (11), pp. 190–201

Kalesnykas, R. (2002). Possibilities to integrate the private security in the system of law and order. *Jurisprudence: Academic Journal of Mykolas Romeris University*, No. 26 (18), pp. 71–82

Kalesnykas, R. (2007). Privatization processes of policing in Lithuania. *SIAK Journal: Zeitschrift für Polizeiwissenschaft und Polizeiliche Praxis*. Wien: Bundesministerium für Inneres, No. 3, pp. 14–24

Kalesnykas, R. (2012). Accountability and integrity issues in public-private security cooperation. In book "Policing and Security: CEPS 2012", 4–5 October 2012. Melbourne, Australia: Centre of Excellence in Policing and Security, pp. 23–28

Miller, L. S., Hess, K. M., Christine, H. (2017). *Community Policing: partnerships for problem solving*. USA, Boston: Cengage Learning

Morabito, A., Greenberg, S. (2005). Engaging the private sector to promote homeland security: law enforcement – private security partnerships. Washington, D.C.: Bureau of Justice Assistance

Mulone, M. (2012). When Private and Public Policing Merge: Thoughts on Commercial Policing. *Social Justice*, Vol. 38 (1–2), pp. 65–83

Nemeth, Ch.P. (2012). *Private Security and the Law*. USA: Elsevier

Prenzler, T., Sarre, R. (2012). Public–private crime prevention partnerships. In book: Prenzler, T. *Policing and security in practice: challenges and achievements*. UK: Palgrave Macmillan, pp. 149–197

Private security and its role in European security (Fifth White Paper, Paris, December 2008). Belgium: CoESS – Confederation of European Security Services, p. 98. Retrieved from http://www.coess.org/newsroom.php?page=white-papers

Private Security services in Europe: CoESS Facts and Figures 2013. Belgium: CoESS – Confederation of European Security Services. Retrieved from http://www.coess.org/newsroom.php?page=facts-and-figures

Sarre, R, Van Steden, R. (2011). The growth of privatized policing: some cross-national data and comparisons*. International journal of comparative and applied criminal justice*, Vol. 31 (1), pp. 51–71

Schaeffer, P. V., Loveridge, S. (2002). Toward an understanding of types of public–private cooperation. *Journal Public Performance & Management Review*, Vol. 26 (2), pp. 169–189

Shared Vision, Common Action: A Stronger Europe. Global Strategy for the European Union's foreign and security policy (2016), accepted in June 2016 by High Representative of the European Union for Foreign Affairs and Security Policy. Retrieved from http://eeas.europa.eu/archives/docs/top_stories/pdf/eugs_review_web.pdf

Sotlar, A., Meško, G. (2008). Police and private security in Slovenia – between conflict, competition, cooperation and partnership. CRIMPREV Symposium "Private policing and security – relationships between the private and public sectors", Ljubljana, University of Maribor, 4–6 December 2008, pp. 7–8. Retrieved from https://www.fvv.um.si/crimprev/abstracts.pdf

Sparrow, M. K. (2014). Managing the boundary between public and private policing. *New Perspectives in Policing Bulletin,* September 2014, Washington, DC: U.S. Department of Justice, National Institute of Justice. Retrieved from https://www.ncjrs.gov/pdffiles1/nij/247182.pdf

Study on the development of statistical data on the European security technological and industrial base (June 2015). The Netherlands, Rotterdam: ECORYS. Retrieved from https://ec.europa.eu/home-affairs/sites/homeaffairs/files/e-library/documents/policies/security/reference-documents/docs/security_statistics_-_final_report_en.pdf

The new security company: integration of services and technology responding to changes in customer demand, demography and technology (Fifth White Paper, Berlin, 23 April 2015). Belgium: CoESS – Confederation of European Security Services, 52 p. Retrieved from http://www.coess.org/newsroom.php?page=white-papers

Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union. Published: Official Journal of the European Union L 194/1 (19.7.2016). Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?toc=OJ:L:2016:194:TOC&uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG

Renewed European Union Internal Security Strategy 2015–2020, approved by the European Council on 10 June 2015, No. 9798/15. Retrieved from http://data.consilium.europa.eu/doc/document/ST-9798-2015-INIT/en/pdf

Regulation (EC) No 300/2008 of the European Parliament and of the Council of 11 March 2008 establishing common rules in the field of civil aviation security and repealing Regulation (EC) No 2320/2002. Official Journal of the European Union, 2008/L 97/72. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32008R0300

Council Recommendation of 13 June 2002 regarding cooperation between the competent national authorities of Member States responsible for the private security sector. Official Journal C 153 (27.6.2002). Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32002H0627%2801%29

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Official Journal of the European Union, 2016/L 119/1. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1528874672298&uri=CELEX%3A32016R0679

Directive 2006/123/EC of the European Parliament and of the Council of 12 December 2006 on services in the internal market. Official Journal of the European

Union, 2006/L 376/36. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32006L0123

Communication from the Commission to the European Parliament, the Council and the European Economic and Social Committee "Security Industrial Policy Action Plan for an innovative and competitive Security Industry", COM/2012/0417 final (26.7.2012). Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2012:0417:FIN

About the Author

Raimundas Kalesnykas, *Prof. Dr.*
Raimundas Kalesnykas is lecturer at the Faculty of Law of the Kazimieras Simonavicius University in Vilnius, Lithuania. He graduated in law and security studies within security manager specialization (BA, Master and PhD) at the Law University of Lithuania. Raimundas Kalesnykas has more than 20 years of professional experience as researcher, academic, trainer (ToT), published more than 50 books and research papers, presented research results over 80 international scientific conferences in Lithuania and abroad, as a invited professor visited over 60 foreign universities for lecturing, successfully implemented over 30 international projects on issues of security and anti-corruption risk management and strategical solutions, police, criminal justice and security sector reform. He has over 14 years' professional experience working as a key security and anti-corruption expert in OSCE, USAID, Saferworld and other international

THE BASIC CONCEPTS AND STYLES OF LEADERSHIP FOR SECURITY SPECIALISTS

Olena de Andres Gonzalez

Introduction

A contemporary organisation embodies a complex system of relations based on the rights and obligations of managers and employees targeted at reaching their shared goals, including the goal of ensuring safety and security of their organisation.

In the global context, leadership has been acknowledged as one of the most effective means of reaction to difficulties faced by companies during their lifetime. Contemporary leadership is increasingly viewed as a desire of a business for a steady development, in a conditions of the globalisation and created by them the socio-economic and ecological risks and opportunities.

A manager of an organization can be a leader for his/her subordinates, but not necessary he/she may be leader too. It is important that security specialists understand that the most effective solution involves a combination of a managerial position with a wisely selected leadership style. Despite the existence of numerous position-related instructions and technical safety regulations, people continue to consciously or subconsciously ignore them. When subordinates viewing their manager not only as an official person but also as a leader, it promotes a more effective compliance with instructions, requests and orders as well as decreases a possibility for dangerous situations. In this study the main goal was to review the basic definitions, theories and concepts of leadership in the context of using the obtained scientific results in the future work of security specialists. In particular, emotional intelligence and transformational leadership styles are analysed, as one of the recommended styles of leadership in security at the moment. To achieve the main goal of study the methods of systematization and generalization of available existing research were used.

1. The definition of leadership. Differences between a leader and a manager

Taking into account the variety of interpretations of the definitions of Leadership and a Leader in various languages, cultures and ages, there are also numerous existing approaches towards defining their meanings. In the context of this chapter we use the following definitions:

Leadership – is an important quality for managerial activities, the key to which lies in an interrelationship between a leader and followers based on an optimum combination of the sources of power and the guidance of followers towards reaching of definite goals.

A Leader – a person in an organization, who is capable of extending influence on other people and directing them towards reaching definite goals.

It is important to note the difference between the roles of a leader and a manager in a company: despite the fact that they can and should be in accord with each other, they are different from the outset. When working with a group of people, a manager essentially relies on the power of authority (official position) assigned by him/her and the sources ensuring it (superior-subordinate relations). Subordinates do not choose their superior and do not confer powers to him/her. A leader generally uses the social basis of power and works with a group of people as with followers (leader-follower relations). A leader is a trusted person, honoured on the basis of qualification, personal charisma or other personality traits, whose values are shared by followers and who will enjoy the support of the group in all his/her activities. Although holding a formal authority position, an entrepreneurial status or an expert position strongly facilitate that a person becomes a leader, however they in itself do not turn anyone into a leader. A person becomes a leader when his/her followers consider him/her as a such and if they are do ready to follow their leader and voluntarily support his/her goals. As it was stated before, the optimum solution lies in the combination of a formal managerial position and the behaviour of a leader. Therefore, for the purposes of further discussion, we shall address a leader as a manager and a leader as an individual in one person.

2. The definition of power, its types and sources

Power is an ability to influence people to perform actions that they would not do without that influence. Power may be present, but not applied actively. Personal power involves good relationship and respect from the group towards a particular person.[179] There are various types of power based on various foundations and the basis of power lies in its source.

The personal basis of power includes the following sources of power[180]:

1) *expert power* – an ability to influence a group on the basis of one’s qualifications and competencies, experience,

[179] Vikhansky, O.S., Naumov, A.I. (2014). *Management,* 5th ed. M: Master, INFRA-M, p. 576

[180] Ibid

education, skills and specialised knowledge. The characteristics of this type of power are related to its narrow area of applicability (only in an area, which is compatible to the respective knowledge) and to the fact that acquisition of those characteristics takes time (it is impossible to become an expert, gain experience and knowledge in a short span of time);

2) *the power of example* – is based on manager's charisma, i.e. on a combination of the strengths of his/her personality and management style. A manager can be liked by a group so much that the group strives to imitate everything the manager is and does, thus empowering the manager over themselves;
3) *the right to power* – an understanding by subordinates that a person holds a top managerial position and possesses a formal power, which they recognise within the boundaries of his/her rights and obligations;
4) *the power of information* – an opportunity to access information, that is necessary and required by others, control of a communication network or part of it, and an ability to use this opportunity for the purposes of influencing subordinates. This represents a very strong source of power and moreover: as opposed to expert power, it does not require knowledge of the subject of control, but the understanding of the value of information is sufficient in this case.

At an organizational level, the sources of powers include[181]:

[181] Vikhansky, O.S., Naumov, A.I. (2014). *Management,* 5th ed. M: Master, INFRA-M, p. 576

1) *decision-making* – resides in the ability to influence any important part of a decision-making process at any time, not just at its final stage;
2) *rewarding* – one of the most widespread sources of power at any organization. Therein, remuneration can be the satisfaction of any necessities of a subordinate at a given point (a bonus payment, a vocation, career growth, etc.). The strength of power depends on a degree of necessity of a subordinate executive in one or another form of rewarding. It is accompanied by the sense of justice within a group, for instance, in cases of an unjust refusal of rewarding or an unjust rewarding for non-compliance with the conditions of a work, the moral authority of a manager declines and the working environment deteriorates;
3) *coercion* – the ability to enforce an employee to implement actions required for a manager under the threat of punishment (penalty, demotion, dismissing). This type of power significantly deteriorates the overall working environment in a collective, it hampers personal initiative of employees and leads to a higher turnover of staff. It is advisable to use this only if one is convinced that the punishment is justified. In that case, it can bring a work collective closer together and can also strengthen the authority of a leader;
4) *control of resources* – to a various extent organizational resources are always limited. By applying control on the distribution of the limited resources, management gains power over those who are in need of those resources, to the extent they are important or desirable to the receiver;

5) *the power of connections* – its essence is based on members of a group believing that their senior management has access to certain people in certain positions and maintains friendly or family ties with them. The characteristics of this type of power is related to the fact that a person may not have real connections, but at the same time, a person can create an impression of existence of this connections thus creating him/her certain power.

3. The concepts of leadership and styles of leadership

Many different concepts have been created throughout the history of leadership studies depending on what exactly lies at the core of the leadership phenomenon. They have been divided into 5 groups, which are referred to as leadership theories or schools (Table 1).

A leadership style represents a quite consistent model of behaviour that characterise a leader[182]. In the contemporary environment, an organization needs leaders who can deliver an effective performance depending on the dynamically changing international environment.[183]

[182] DuBrin, A. J. (2001). *Leadership: Research findings, practice, skills*, 3rd ed. Boston: MA, Houghton Mifflin, p. 487

[183] CISL (2017). *Global Definitions of Leadership and Theories of Leadership Development: Literature Review*. Cambridge: Cambridge Institute for Sustainability Leadership

Table 1

General theories of leadership[184]

Theory/school and description	**Main representatives**

Great Man or Trait school. Celebrates outstanding individual leaders (in the heroic tradition) and studies their traits or characteristics to understand their accomplishments as leaders.	Stodgill, 1948;
	Tannenbaum and Schmidt, 1973;
	CEML, 2002;
	Harter, 2008

Behavioural or Styles school. Describes leadership in terms of people- and task-orientation, suggesting that different combinations of these produce different styles of leadership.	Lewin et al., 1939;
	Blake and Mouton, 1964, 1985;
	Kouzes and Posner, 1995

Situational or Context school. Emphasises the importance of context in shaping leaders' responses to be more relationship or task motivated, or more authoritative or participative.	Hersey and Blanchard, 1969, 1974;
	Vroom and Yetton, 1973;
	Graeff, 1983

Contingency or Interactionist school. Proposes that leaders' influence is contingent on various factors (like positional power), which in turn determines appropriate leadership styles.	Fiedler, 1967;
	House and Mitchell, 1974;
	Barbour, 2008

Transactional or Transformational school. Contrasts leadership as a negotiated cost-benefit exchange and as an appeal to self-transcendent values of pursuing shared goals for the common good.	Bass, 1974;
	Burns, 1978;
	Price, 2003

In the course of many years studies have been conducted, and various models of effective leadership have been developed. At first it was thought that one could find a universal style, applicable

[184] CISL (2017). *Global Definitions of Leadership and Theories of Leadership Development: Literature Review*. Cambridge: Cambridge Institute for Sustainability Leadership

to any organization in any situation. Contemporary studies claim that leadership styles should be chosen on the basis of a situational context and something that may work well in one situation may be completely inapplicable in another. It is exactly why the behaviour of a leader must be flexible and adaptable.[185] Allio and Gordon in their studies describe that a contemporary employee of a contemporary organization expects cooperation from a leader and not just use of power[186, 187].

4. Emotional intelligence

The concept of Emotional Intelligence developed by Daniel Goleman in the middle of the 1990's became on the most popular concepts in this area. He concluded that emotional intelligence is based on 5 key components: self-awareness, self-regulation, motivation, empathy and social skills. Besides, Goleman has established that it is exactly these components that in the aggregate help us manage ourselves and our relations with people around us in an effective way. In 2000 Goleman described 6 leadership styles (Table 2) based on emotional intelligence and established as a result of studies conducted by Hay/McBer consulting company[188].

[185] Gordon, A., Yukl, G. (2004). The future leadership research: challenges and opportunities. *German Journal of Human Resource Research*, No. 18(3), pp. 359–365

[186] Allio, R. J. (2009). Leadership – the five big ideas. *Strategy and Leadership*, No. 37(2), pp. 4–12

[187] Gordon, A., Yukl, G. (2004). The future leadership research: challenges and opportunities. *German Journal of Human Resource Research*, No. 18(3), pp. 359–365

[188] Goleman, D. (2000). Leadership that Gets Results. *Harvard Business Review*, March–April, pp. 78–90.

Table 2

Leadership styles according to D. Goleman[189]

	Coercive	Authoritative	Affiliate	Democratic	Pacesetting	Coaching
The leader's modus operandi	Demands immediate compliance	Mobilizes people towards a vision	Create harmony and builds emotional bonds	Forges consensus through participation	Sets high standards for performance	Develops people for the future
The style in a phrase	"Do as I say."	"Come with me."	People come first."	"What do you think?"	"Do at my pace."	"Try this."
Underlying emotional intelligence competencies	Drive to achieve, initiative, self-control	Self-confidence, empathy, change catalyst	Empathy, building relationships, communication	Collaboration, team leadership, communication	Conscientious, drive to achieve, initiative	Developing others, empathy, self-awareness
When the style works best	In a crisis, to kick-start a turnaround, or with problem employees	When changes require a new vision, or when a clear direction needed	To heal rifts in a team or to motivate people during stressful circumstances	To build buy-in or consensus, or to get input from valuable employees	To get quick results from a highly motivated and competent team	To help an employee improve performances or develop long-term strengths

The *Coercive Style* must be applied only upon necessity. He demonstrates a clear hierarchy and application of power in a "downwards targeted" pattern. It generally has a negative effect on the environment of a work collective by lowering the spirit of initiative, motivation and the level of personal responsibility. It is preferable to use this style only in crisis situations and upon necessity, for instance, in situations require fast decision-making.

The *Authoritative Style* should be applied in situations where it is necessary to demonstrate employees a new vision, to inspire them and to explain them a new direction their company is taking. According to the Goleman's studies, it has been accepted as one of the most effective styles. This style inspires people because employees

[189] Goleman, D. (2000). Leadership that Gets Results. *Harvard Business Review*, March–April, pp. 78–90

see that their actions are an integral part of the common vision and development of an organization. Additionally, employees have enough room for independent action. It has a highly positive impact on the internal environment of a work collective.

The *Affiliative Style* promotes the establishment of emotional bonds with employees. A leader shows that he/she values human emotions higher than organizational goals, notices their results and pays attention to each employee. It is good to apply this style when employees are under stress and are in need of a “parent-like” support of their leader. This style leads to substantial improvement of the working environment. However, due to its low goal-orientation level, it does not contribute to reaching ambitious goals of a company.

The *Democratic Style* presupposes that a leader expects engagement of employees and a collective decision-making. When a leader requires new goals, he/she demonstrates the value of thoughts and input of employees and thinking out of the box. It has a positive general impact on the work environment. Unfortunately, this style requires too much time to make it a permanent. It also requires highly qualified employees and leader's capacity to conduct discussions.

In the framework of the *Pacesetting Style*, a leader establishes extremely high standards for his team. A leader demonstrates the ways of reaching those high standards on the bases of a personal example, while at the same time he/she does not notice small successes of employees and harshly criticises them for bigger and smaller mistakes. This usually leads to worsening of the work environment, lowering of individual initiative of employees, deterioration of trust and loyalty and loss of personal independence. This style works exclusively for highly qualified and motivated teams who solely need a general direction related to main tasks.

The *Coaching Style* promotes professional development of employees, and it is oriented towards defining the long-term professional goals of people. A leader happily delegates authority, entrusts employees with important duties and provides feedback. It has a highly positive impact on the work collective, promoting the development of an organization and individual development of employees. However, it encountered extremely rarely, since a leader has not enough time to pay so much attention to employee training.

Goleman recommends management practitioners to continuously broaden their set of leadership styles and to study the key components of emotional intelligence internally as well as in the people around.

According to studies conducted by EU-OSHA[190], the use of emotional intelligence theory in the work of security experts can play a highly positive role on work collectives and the level of security in general. The use of emotional intelligence raises the level of action awareness and their consequences by employees and as a result creates a more positive attitude towards security and of an enterprise; assists in the prevention of “bullying” in a work collective; helps to improve the atmosphere in a workplace; raises the effectiveness of labour safety measures; increases productivity; develops internal personal intelligence, which lets security experts keep a positive mindset and overcome work-related difficulties; develops interpersonal intelligence, which assists in more effective communication with employees and encourages them to a safer behaviour.

[190] Kaluza, S., Hauke, A., Starren, A., Drupsteen, L., Bell, N. (2012). Leadership and Occupational Safety and Health (OSH): An Expert Analysis. s.l.: European Agency for Safety and Health at Work

5. Transformational leadership

In transformational leadership style a leader inspires employees to pursue positive changes targeted at optimisation of their work by means of raising their motivation, morale and productivity.[191]

Transformational leadership is characterised by four behavioural aspects:

1) idealised influence: a leader must be a model for imitation and should demonstrate high moral and ethical principles and ideals. Due to the fact that people trust their leader and respect him/him, they tend to adopt his/her behavioural and thinking patterns and try to imitate that leader;
2) inspirational motivation: a leader motivates followers by demonstrating a clear vision of goals and optimism for reaching them, by setting realistic and applicable tasks and standards. When a person works with this type of leader, he/she gets inspired for the fulfilment of one's duties, believes in him/herself, becomes increasingly goal-oriented and wants to meet the expectations of that leader;
3) intellectual stimulation: a leader presents challenging tasks and possible difficulties as opportunities for learning and personal growth, a leader inspires co-workers for a creative approach and innovative solutions;
4) individualised consideration: a leader pays attention to the individual needs of followers. By employing individual coaching, mentoring and smart tasking, a leader supports individual growth of each employee and strives to expand

[191] Kaluza, S., Hauke, A., Starren, A., Drupsteen, L., Bell, N. (2012). Leadership and Occupational Safety and Health (OSH): An Expert Analysis. s.l.: European Agency for Safety and Health at Work

opportunities of his/her followers by harmonising goals of an organization with individual needs of persons. This kind of leader is always open to communication and he/she possesses interpersonal communication skills.

Contemporary studies have proven a link between transformational leadership and security. Conclusions of European Agency for Safety and Health at Work refer to studies, that argue that the transformational leadership style can be applied in the work of security experts, in order to motivate employees towards reaching goals of an organization as well as personal goals, including goals focusing on using additional measures for securing a working environment[192]. As a result of their studies, Pilbeam, Davidson, Doherty and Denyer have come to the conclusion that transformational leadership increases employee engagement in ensuring company security. By creating a favourable atmosphere and the necessary level of trust this style of leadership contributes to decreasing of accidents and increasing the overall security and safety by engaging employees in implementing the overall security policy.[193]

[192] Kaluza, S., Hauke, A., Starren, A., Drupsteen, L., Bell, N. (2012). Leadership and Occupational Safety and Health (OSH): An Expert Analysis. s.l.: European Agency for Safety and Health at Work

[193] Pilbeam, C., Davidson, R., Doherty, N., Denyer, D. (2016). *Safety leaders: who are they? What do they do?* Cranfield University – School of Management. LE, Wigston: IOSH, p. 60

6. The principles of leadership in security

Studies of European Agency for Safety and Health at Work recommends the following five principles for leadership in security[194]:

1) leaders must treat their responsibilities regarding the implementation of a positive culture on security issues at their company with utmost seriousness. For this purpose, they should employ an optimum combination of leadership styles and should take into account individual characteristics of the particular group;
2) leaders need to establish definite security as a priority in reaching the overall goals of a company;
3) leaders and senior managers must engage directly in the implementation of an effective security policy at a company;
4) leaders and senior managers must develop high-quality multilevel communications. For this purpose, it is necessary to support a friendly and open environment, promote sharing of experience among employees, open expression of ideas related to the improvement of security policy;
5) leaders must reward employees for active participation in improvement and implementation of security policy measures at a company and must show that their input is highly regarded at a company level.

[194] Kaluza, S., Hauke, A., Starren, A., Drupsteen, L., Bell, N. (2012). Leadership and Occupational Safety and Health (OSH): An Expert Analysis. s.l.: European Agency for Safety and Health at Work

Conclusion

The study summarizes and systematizes the main concepts of leadership, describes difference between leader and manager, shows types of power and its sources, presents the basic theories of leadership and the recommended principles of leadership for security professionals. Based on the analysis, it was revealed that in the field of security it is currently recommended to use leadership based on emotional intelligence and transformational leadership. These styles have a very positive impact on the team, reducing the number of accidents and increasing the involvement of employees in the process of ensuring the security policy in the enterprise. Enforcement is no longer perceived as an adequate behaviour of a senior manager. A leader should employ effective communication skills, empathy, emotional and social intelligence, systemic thinking, knowledge of a situation and personal engagement. Moreover, a leader feels oneself part of a group, sharing the decision-making process with other employees and performs management actions from the inside by using the most applicable situation and context-dependent styles of leadership. A contemporary leader understands responsibility not just as securing strategic and operational goals of a company, but also as an important contribution to the development of society, preservation of the environment, ensuring comfortable and safe working conditions, providing opportunities for professional and personal growth, as well as for the health of employees.

References

Allio, R. J. (2009). Leadership – the five big ideas. *Strategy and Leadership*, No. 37(2), pp. 4–12

Bass, B. M., & Riggio, R. E. (2006). *Transformational leadership,* 2nd ed. Mahwah, NJ: Lawrence Erlbaum Associates

CISL (2017). *Global Definitions of Leadership and Theories of Leadership Development: Literature Review.* Cambridge: Cambridge Institute for Sustainability Leadership. Retrieved 10.05.2018 from https://www.britishcouncil.org/sites/default/files/final_leadership_literature_review.pdf

DuBrin, A. J. (2001). *Leadership: Research findings, practice, skills,* 3rd ed. Boston: MA, Houghton Mifflin

Goleman, D. (2000). Leadership that Gets Results. *Harvard Business Review*, March–April, pp. 78–90

Gordon, A., Yukl, G. (2004). The future leadership research: challenges and opportunities. *German Journal of Human Resource Research*, No. 18(3), pp. 359–365

Kaluza, S., Hauke, A., Starren, A., Drupsteen, L., Bell, N. (2012). *Leadership and Occupational Safety and Health (OSH): An Expert Analysis. s.l.*: European Agency for Safety and Health at Work. Retrieved 10.05.2018 from https://osha.europa.eu/en/tools-and-publications/publications/literature_reviews/leadership-and-occupational-safety-and-health-osh-an-expert-analysis

Pilbeam, C., Davidson, R., Doherty, N., Denyer, D. (2016). *Safety leaders: who are they? What do they do?* Cranfield University – School of Management. LE, Wigston: IOSH, 60 p.

Vikhansky, O. S., Naumov, A. I. (2014). *Management*, 5th ed. M: Master, INFRA-M

About the Author

Olena de Andres Gonzalez, *PhD*
PhD degree in Economics and Management of Enterprises from Institute of Economics of National Mining University in Ukraine since 2015.
From 2007 she was engaged in teaching activities and conduct lecturer and seminars within Foundations of Management, Leadership, Conflict Management, Business Planning, Strategic Management and Project Management courses. Olena had hold a position of Assistant Professor and Deputy of Dean for Educational Affairs of the Faculty of Management in Institute of Economics of National Mining University in Ukraine for two years. From May 2017 she had internship and now works at University of Turku, Turku School of Economics Pori Unit, Finland as a project researcher.

PROFESSIONAL ETHICS

Ivita Kīsnica

Introduction

People generally choose to trade some aspects of personal freedoms for the good of social order. The balancing of the individual self-determination rights of the members of the public with the needs of society as a whole is called laws. Laws are regulations, which authorise or prohibit certain behaviour; they are based on ethics, which determines a socially acceptable behaviour. The main difference between laws and ethics lies in the fact that laws contain state administration authority, while ethics does not. Ethics in its own turn is based on cultural heritage: certain groups gave certain moral attitudes or conventions. Some ethical standards are universal. For instance, murder, theft, assault or arson are actions, which are not in line with ethical and legal acts around the world.[195]

Professional ethics is a sub-type of general ethics encompassing the obligations of a professional role. Professional ethics prompts and supports those values and norms, which defend the inviolability of both state and private property and prestige, while simultaneously promoting the development of an employee as a personality, sustaining his/her self-respect and inherent value based on his/her commitment, responsibility and self-dependency. The rise of such laws and norms testify of the positive traits in the moral progress of the humanity because they are related to the rise in the value of a personality and humanity in mutual relations.

[195] Whitman, E. M., Mattord, J. H. (2011). *Principles of information security*. Cengage learning, p. 89

Ethics deters a person from an unreasonable action in which career propensities and seeking of self-interest at the expense of others can harm a person him/herself, the general public and the state. Ethics also encompasses well-being of a personality, which is not always considered as a value in a work process.

The key characteristics of professional moral of a personality are:

1) attitude towards work;
2) professionalism;
3) the norms, behaviour and work culture of an expert, ideals;
4) ethical, professional values characteristic to the respective profession, moral characteristics, which ensure the performance of professional duties.[196]

Therefore, on the one hand the focus of attention of professional ethics includes improvement of professional ethical competences of experts, the specifics of professional education of a personality and regularities of moral development of each individual expert, while on the other hand: mutual relations within groups (supervisor and subordinate relations, relations among colleagues, relations with a professional subject, e.g., teacher-pupil, coach-trainee, lecturer-student, etc.).[197]

Professional ethics normally addresses the following phenomena:

1) conflicts of interest, discrepancies;
2) relations with people around;
3) individual responsibility and freedom of action;
4) basic moral commitments.

[196] Kuzņecova, A. (2003). *Profesionālās ētikas pamati*. Rīga: RAKA, p. 34

[197] Ibid

All these phenomena form the basis of codes of ethics. All the phenomena are interrelated because they are on the basis of the daily life of employees. Compliance with basic obligations positively affects relations with people around, facilitates the most viable resolution of disagreements, and promotes reasonable decision-making. If ethical awareness is functioning, there is no need for bodies of legal norms, regulating public relations.

The functions of professional ethics are:

1) resolution of problems, which are not regulated by law (on justice);
2) to streamline relations between professionals and clients;
3) non-disclosure of professional secrets to the third parties (the principle of confidentiality);
4) to define the principles of operation (the basic unifying principles of all codes of ethics: independence, honesty, justice, trust, the principle of confidentiality).

There is a necessity for ethics in all areas, including entrepreneurship, it is unavoidable. Generally ethics is one of the cornerstones of entrepreneurship regardless if an entrepreneur is engaged in security guard business, wholesale, represents health and beauty industry or is engaged in individual commerce, since ethics involves practical considerations, experience and contemplation on the ways of optimising relations in the work environment and how to gain sense in that sphere, which occupies a large part of human life, i.e., professional performance. Professional ethics pays attention to those situations which reveal moral obligations in attitudes towards a state, a company, an institution, colleagues, visitors, towards work in general and finally towards oneself.

1. Ethics in the actions of a security representative

Entrepreneurship is defined as an independent and systemic activity of a legal person, which, by assuming risks, undertakes in the area of production of goods or services and which is targeted at gaining profit.[198]

Entrepreneurship is a lifeblood of market economy, which provides money (taxation) to state institutions, the areas of education, culture, etc. It has an enormous impact on the development of society.[199]

The specifics of entrepreneurship are determined by the fact that, in contrast to medicine or pedagogy, it is oriented egoistically. Its ultimate goal is maximum profit, which is the source of welfare not only for an entrepreneur but for society as a whole. It is also the basis of development of entrepreneurship and society. Striving for gaining maximum profit, each person engaged in entrepreneurship is bound to cooperate with other actors. Employers and employees, producers and consumers, customers and sellers, suppliers and contractors become participants of such cooperation. Despite their cooperation, they are also competitors: an employer wishes to contract the best employees for the lowest salary, an employee: to sell one's labour at a higher price and to get better work conditions, customers wish to buy better goods at lower prices while sellers wish to sell more at higher prices, etc.[200]

[198] LZA terminoloģijas komisija (2018). *Akadēmiskā terminu vārdnīca*. Retrieved from http://termini.lza.lv/term.php?term=uz%C5%86%C4%93m%C4%93jdarb%C4%ABba&list=uz%C5%86%C4%93m%C4%93jdarb%C4%ABba&lang=LV

[199] Rogenbuka, I. (1999). *Uzņēmējdarbības ētika*. Rīga: Zvaigzne ABC, p. 5

[200] Ibid, p. 7

In order to maximise profit, entrepreneurs must think in broader terms, they must cooperate with various representatives of the public. They also have to think about ways of providing maximum security to their activities. Security from various points of view.

For a company to operate successfully and safely they must put maximum effort at avoiding not only economic risks related to buying and selling but also security risks, for instance, possibilities of theft, unsanctioned access to their premises or other activities leading to losses. For this purpose, companies often create their internal security service, engage a company providing security services or contract an individual security guard who ensures the operation of a security guard service.

Operation of a security guard service: installation of technical security systems, providing of security guard services for cargoes, goods or other movable property, guarding of ready money or securities and physical persons, safeguarding of internal order and security at objects under protection, providing of security guard consultations as well as other activities or an aggregate of activities performed by a security guard, security service entrepreneur or internal security service in order to prevent illegal or other threats to object under protection.[201]

The type of service chosen by an entrepreneur mostly depends on the scope of work and one's paying capacity.

Employee of a security guard service: a physical person, who has received a security guard certificate and performs security guard activities[202] regardless if a person works for a particular security service guard entrepreneur (a commercial operator who

[201] Apsardzes darbības likums. Adopted on 13.02.2014. *Latvijas Vēstnesis*, 06.03.2014, Nr. 37. Latest amendments 19.01.2017, p. 1

[202] Ibid, article 1, sub-point 2

has received a special permit (licence) for performing security guard service operations) or for an internal security service (a structural unit of an institution, a commercial entity or an organization, which provides its security guard services, internal order and security) and is an important part of a company. There are companies where a security guard service employee is their top official, who also meets visitors. There are companies, where the presence of a security guard is visible and operates only in emergency situations, mostly remaining invisible to visitors. Regardless of specific duties and role of a particular security service employee at a company, when coming into contact with a person visiting a particular company, a security guard/security representative also participates in forming company's overall image. The overall image is formed not only by a dress code in place but also by physical condition, behaviour (ethical or non-ethical). In this case, it is a secondary issue whether a company has its own security service, its own security guard or they use an outsourced provider. A particular security service employee gets associated with a particular company where he is present and performs his duties.

Ethics refers to the principles of right and wrong that individuals, acting as free moral agents, use to make choices to guide their behaviours.[203]

Many professional groups have their own clear regulations governing ethical conduct in a workplace. For instance, doctors and advocates who have conducted serious professional breaches can lose their rights to practice. However, compared, for instance, to medical and legal professions, the area of information technology,

[203] Devendra Kumar Tiwary (2011). Security and ethical issues in it: an organization's perspective. *International Journal of Enterprise Computing and Business Systems*. Vol. 1, Issue 2, July 2

particularly IT security does not contain a binding code of ethics. Other security-related sectors may have developed codes of ethics, which include ethical processes and breach of those codes can lead to disciplinary action or other forms of liability.

Several professional organizations have established their codes of ethics or codes, by which their members should abide. Codes of ethics can positively affect judgement of people regarding representatives of the security sector. The duty of security experts is to act in an ethical manner and in compliance with legal enactments and procedures established by their employers, professional organizations and public legislature in general. An organization is also responsible for the development, dissemination and enactment of its policies.[204]

The Code is intended to serve as a user-friendly guide for staff and managers to use in day-to-day interactions and decision-making, consistent with our Mission, Guiding Principles, and Core Values. It does not purport to contain all the answers, and does not address every ethical issue that staff may face. The Code is not a substitute for good judgement, nor does it replace or supersede the Principles of Staff Employment, the Staff Rules, and other applicable principles, rules and guidelines. Rather, it serves as a bridge between our aspirations and operational realities, and speaks to the spirit of our commitment to our Mission. The Code is also a tool to encourage discussion of ethics and to improve our response to work-related ethical dilemmas and uncertainties.[205]

[204] Whitman E. M., Mattord J. H. (2011). *Principles of information security*. Cengage learning, p. 90

[205] *Code of professional ethics* (1999). The World Bank Group, p. 3

However, regardless of the level of detail ethical principles are reflected in a code, it is impossible to define everything. Ethical breaches take place also among the security service personnel. Those breaches are not only related to relations with colleagues and visitors of a company if contacts with them are in line with work requirements. There are occurrences of much more serious violations against employers. Corruption is one of such violations.

Honesty is one of the fundamental values of ethics. We all make hundreds of decisions each day. Some of their consequences are small. Others are enormous and affect people whom we may never meet. In part, we base our decisions on information that is available to us.

Corruption is one of the gravest, if not the gravest, ethical violations.

Various definitions are used for the purpose of explaining corruption. Social sciences broadly use the definition by Colin Nye: "Corruption is a behaviour that deviates from the formal duties of, a public role (elective or appointive) because of private-regarding (personal, close family, private clique) wealth or status gains". Sociologists explain that corruption is a refusal of representatives of power to implement a standardised (definite) behaviour for reason of illegal personal gain. The Council of Europe provides one of the most precise interpretations of corruption by stating that corruption is bribery and any other action of those persons entrusted with responsibility in the public and private sector and who are in breach of their responsibilities resulting from their status of a public official, independent entrepreneur or any other form of relations and which is targeted at gaining an undeserved privilege for himself/herself or others.[206]

[206] The Corruption Prevention and Combating Bureau. (2018). Corruption. Retrieved on 12.05.2018 from https://www.knab.gov.lv/lv/education/forschools/

According to the definition of the Council of Europe, corruption exists in both: public and private sectors. In the public sector, corruption is understood as bribery or any other action by a public official targeted at gaining undeserved privilege for himself/ herself or other persons by means of using one's official status and authority or by abusing those powers. When explaining corruption in the public sector it is important to keep in mind three characteristics: (1) public official, (2) use and abuse of the official status and authority, as well as (3) undeserved privilege.[207] Corruption is punishable under criminal law.

Today ethics, fight against corruption and practice of corporate governance are the three key considerations in business decisions related to competitive advantage and financial results. Ten years ago the picture was completely different. Even in the best scenario, these themes were considered as unfair non-financial issues and in the worst case, they were dismissed or dismissed on the bases of non-compliance with the basic goal of profit. Today companies representing all industries, sizes and regions of the world can easily include these issues as strategic components of sustainable long-term business development. The shift of non-financial issues from optional to key components of decision making in business is one of the most important changes, which we can achieve. The consequences of this shift as well as the statement used in its development will be significant for the world future in terms of economic integration, national development and reduction of poverty. Today we possess a strong and practical set of tools: the guidelines on good corporate governance, which did not exist ten years ago. Moreover, taking into the account the increased understanding

[207] The Corruption Prevention and Combating Bureau. (2018). Corruption. Retrieved on 12.05.2018 from https://www.knab.gov.lv/lv/education/forschools/

of the corporate world and its desire to engage in the good governance programme, there is also an increased unanimity supported by international conventions and national legal acts. The global economic integration has been a driving force of a rapid progress in the development and dissemination of good corporate governance practices and standards. Improvement of good governance is a never-ending challenge with an unrestricted place for innovation, and we are developing and broadening assessment criteria of higher corporate governance standards and ethical values.

A big role, if not the biggest role, in safeguarding any ethics process belongs to a head of a security service or to persons responsible for the company security personnel.

2. The role of a security manager in safeguarding ethics

Ethics literally starts at the top of an organization and cascades down. Thus, security managers often find themselves having to decide between “what my boss is telling me to do and what I know is right.” Security managers are often put in situations in which they are being asked to complete a potentially unethical assignment or ignore an obvious ethical violation at the direction of senior management. Security managers must thus understand their values and how their personal ethics align with a potential employer. Such internal reflection may be facilitated through ethics-related concepts in security management education.

On any given day heads of security must be and they are ready to guard and react to numerous breaches of ethics in companies/ organizations. Ethical issues like employee theft, internal fraud, transmission of incorrect access data and bribery on abuse of internal information, corruption and other issues which a head of security often needs to address on a daily basis by finding justice and preserving company's reputation.

Head of security must comply with ethics management and security decisions in a) investigating breaches of ethics, b) protecting of personnel and assets and c) planning and coordinating of crises responses. Poor ethical decisions of security managers can lead to security breaches, crisis factors and unethical behaviour, posing a threat to organizational stability and increasing chances for organization's possible civil liability.[208]

Although ethical principles and knowledge of ethics are highly important in the daily work of security managers, ethics and education ensure the basis for the progress of security management towards its acceptance as a profession. Professional security organizations, for instance, ASIS International, International Film Protection Foundation and Security Institute work actively in order to raise the professional reputation of security management. However, there are few studies addressing the role of ethics in security management as a practice and a profession.[209] As a subject of research ethics becomes topical not only in the USA but also in Europe, including Latvia, Lithuania and Finland where despite the slightly different local accents and issues, there is a clear unity of views on the need for ethics for company reputation and stability.

Every security function is built on the presumption of trust, and that trust does not exist without ethical decision making by organizational security personnel.[210]

[208] Daniel A. (2013). Ethics in Security Management: Development of a Theoretical Model. *Journal of Applied Security Research*, 8:1, p. 44

[209] Ibid

[210] Ibid, p. 48

Security personnel conduct background investigations, protect executives, investigate internal fraud, plan crisis responses, ensure physical security systems are protecting workers and assets, and myriad other duties, which place them in the public spotlight and require enhanced authority and access to information. Further, no clearly defined set of laws limits the actions of security personnel, unlike their counterparts in public law enforcement who are subject to the criminal justice system of checks and balances to minimize unreasonable infringement of rights.

Regardless of the role the security manager is performing, this different research showed an increased likelihood of the need for ethical decision making as well as heightened consequences for ethical failure. All of the consequences, however, stem from the loss of trust for the security manager or security department by the public, organizational leadership, or workers. Consequences include financial loss for the organization, physical harm to workers, civil liability, reduced revenue, dissolution of the security department, and removal of the security manager upon loss of trust. The aforementioned characteristics of security positions and the significant consequences for ethical failure only serve to reinforce the importance of ethical decision making among security managers.[211]

Organizational Liability and the Need for Counsel

What if an organization does not demand or even encourage strong ethical behaviour from its employees? What if an organization does not behave ethically? Even if there is no breach of criminal law, there can still be a liability. Liability is the legal

[211] Daniel A. (2013). Ethics in Security Management: Development of a Theoretical Model. *Journal of Applied Security Research*, 8:1, p. 53

obligation of an entity that extends beyond criminal or contract law; it includes the legal obligation to make restitution or to compensate for wrongs committed. The bottom line is that if an employee, acting with or without the authorization of the employer, performs an illegal or unethical act that causes some degree of harm, the employer can be held financially liable for that action. An organization increases its liability if it refuses to take measures known as due care. Due care standards are met, when an organization makes sure that every employee knows what is acceptable or unacceptable behaviour, and knows the consequences of illegal or unethical actions.[212] Quite often it is a responsibility of a manager. Safeguarding employee feedback for the purpose of addressing consequences and establishing responsibility is an important factor in the elimination of unethical behaviour in future.

Another problem lies in the fact that the increasing globalisation submits security managers to substantial normative value differences among various cultures. Today security managers encounter complex ethical scenarios in an environment, where an ethical dilemma even cannot constitute an ethical breach in a country or culture of the security manager's current location. The more important place a security manager occupies in an organization, the more important ethics becomes.

Ethics are arguably more important to security managers than to other organizational managers for several reasons:

1) although security personnel have similar authority to law enforcement within an organization, they are not bound by the same laws and restrictions that limit law enforcement. Thus, organizational security personnel are

[212] Whitman, E. M., Mattord, J. H. (2011). *Principles of information security*. Cengage learning, p. 90

required to exhibit ethical discretion for reasons other than legal limitations;

2) security managers have access to employee personal information;
3) as internal investigators, security managers often serve as the ethical example within an organization;[213]
4) ethical failures by security managers can negatively affect the public's perception of the organization;
5) security managers reduce loss through ensuring organizational functionality and maintaining the integrity of human capital as well as other organizational assets;
6) security managers model ethics for security workers and train them on matters related to ethics in security;
7) security is viewed as a cost centre instead of a profit centre. Thus, security managers find themselves justifying the existence of the security department because no profit is gained as a result of the department, and the cost savings produced by security are often not immediately quantifiable. If senior executives perceive the security entity to be of suspect ethical fibre, they will cut off funding because of the necessity for the aforementioned trust. Thus, ethical knowledge and action among security managers is indeed a tangible necessity for career survival;
8) a security manager's success depends upon reputation both among organizational leadership and among organizational workers. Ethical failures interfere with security managers' ability to be relied upon with people's personal information, with company secrets, with people's

[213] Daniel A. (2013). Ethics in Security Management: Development of a Theoretical Model. *Journal of Applied Security Research*, 8:1, p. 51

safety, or during investigations, to be trusted with the truth from witnesses;

9) athical infractions resulting in failed emergency response or security measures can result in injury or death, as well as civil liability and negative press.
10) security managers' duties as investigators, organizational representatives, and gatekeepers to organizational information and resources make them more likely to face situations, which may tempt them to make unethical decisions.[214]

These and many more substantiations point to the importance of ethics among employees as well as point to the responsibility of managers and the importance of ethics in reaching strategic goals of any organization.

Conclusion

Representatives of various professions face increasingly high demands in terms of ethics, which are based on such principles as openness, accountability, transparency, and objectivity. Public expects that professionals of security areas, while performing their duties, will consider public interests as a priority. Ethics deters a person from an unreasonable action in which career propensities and seeking of self-interest at the expense of others can harm a person him/herself, the general public and the state. The development, compliance and control of high ethical standards should therefore be prioritized in each company, thereby contributing to

[214] Daniel A. (2013). Ethics in Security Management: Development of a Theoretical Model. *Journal of Applied Security Research*, 8:1, p. 51

the loyalty of the company`s employees to the company, as well as by promoting a positive external theme and look for the company and to guarantee its customers` confidence in the company. Ethics and trust in the company and its prosperity often go hand in hand, therefore the amount of attention given to ethics should be equal to the amount of attention given to company`s prosperity.

References

Code of professional ethics (1999). The World Bank Group, p. 23

Daniel Adolf (2013). Ethics in Security Management: Development of a Theoretical Model. *Journal of Applied Security Research*, 8:1, p. 60

Devendra Kumar Tiwary (2011). Security and ethical issues in it: an organization's perspective. *International Journal of Enterprise Computing and Business ting and Business ting and Business ting and Business Systems*. Vol. 1, Issue 2, July 2

Kuzņecova, A. (2003). *Profesionālās ētikas pamati*. Rīga: RAKA, p. 202

Rogenbuka, I. (1999). *Uzņēmējdarbības ētika*. Rīga: Zvaigzne ABC, p. 93

Whitman, E. M., Mattord, J.H. (2011). *Principles of information security*. Cengage learning, p. 623

Apsardzes darbības likums. Adopted on 13.02.2014. *Latvijas Vēstnesis*, 06.03.2014, No. 37. Latest amendments 19.01.2017.

The Corruption Prevention and Combating Bureau (2018). Korupcija. Retrieved from https://www.knab.gov.lv/lv/education/forschools/

LZA terminoloģijas komisija (2018). Akadēmiskā terminu vārdnīca. Retrieved from http://termini.lza.lv/term.php?term=uz%C5%86%C4%93m%C4%93jdarb%C4%ABba&list=uz%C5%86%C4%93m%C4%93jdarb%C4%ABba&lang=LV

About the Author

Ivita Kīsnica, MPA
Education: Master degree of Public Administration. Currently a doctoral student in Law Siences study program at the Turiba University.
Work experience: Vice-dean of Faculty of Law in Turiba University. Director of the programme of first level of professional study programme "Law Science" in Turiba University. Lecturer in study course "Professional ethic" and "Professional ethic and presentation". Previous Head of the Business Education Centre; Head of Department of Law Science in turiba University.

Part III

Security threats

VIOLENT EXTREMISM AND RADICALISATION

Tuomas Tammilehto

Introduction

Regardless of the actual likelihood of becoming a victim of terrorism, the risk itself has been for long something that both individuals and organisations are expected to take into account. Whether it is about muddling through the mundane life, for example, participating in mass events, shopping, travelling, or about more serious business, e.g. assuring that uncertainties does not deflect the endeavour from one's business goals, terrorism needs to be dealt at least on intellectual or emotional level, if not in action. To put it short: terrorism has been with us for long, and most likely continues to be an issue, and thus needs to be reconsidered as a phenomenon affecting everyday life.

In addition to terrorism, especially after the rise of the so-called Islamic State (IS), radicalisation and violent extremism have become more prevalent in both popular and security discourses. For example, The New York Times published 104.014 articles from Jan 1, 1851 to Dec 31, 2017 in which according to their search engine the word "terrorism" was mentioned; 1.498 articles with the word "radicalization" (and 22 with "radicalisation"); and 1.473 articles mentioned "violent extremism". Correspondingly, during 2012–2017, the amounts of articles using the same words were 15.245 times "terrorism", i.e. 15 % of the search hits were from past five years; 688 hits of radicalization (+12 radicalisation); and 654 of "violent extremism". During the last five years, the numbers of both radicalisation and violent extremism are significantly lower than those of terrorism, but in percentage they represent almost half of the articles ever published on radicalisation (47 %) and violent extremism (44 %). This is an indication of the rising popularity of the term, despite some methodological problems, such as not being able to trim down the statistics of possible duplicates and/or articles that mention (as so often) all three terms. (https://query.nytimes.com) The Google Scholar (www.scholar.google.com), i.e. the freely accessible web search engine that indexes the full text or metadata of scholarly literature across an array of publishing formats and disciplines reveals, that during between 1851 and 2017 there were ca. 794.000 mentioning of "terrorism"; 45.500 hits with "radicalisation OR radicalization"; and 15.900 hits when using "violent extremism". During the past five years, however, there has been a visible change in the focus of academic literature, at least in the numbers of articles published using the above mentioned terms. 192.000 articles returned from the search engine when using the word "terrorism", i.e. almost one quarter of all articles are published during the past five years; correspondingly 21.300 articles with the search words "radicalisation OR radicalization", again nearly half of the articles (47 %); and 12.300 articles on "violent extremism", thus over two thirds (77 %) of articles have been written very recently. The numbers cannot fully be trusted, since Google does not disclose their algorithms. Nevertheless, the trend is clearly visible even with incomplete data.

Radicalisation and violent extremism have entered into various new domains where terrorism was previously the central problem, and beyond. Radicalisation and violent extremism are actively discussed, for example, in schools and educational institutions, public health sector, social services, and correctional services, just to mention few (For example in the United Kingdom, there are several state level initiatives on preventing radicalisation in different domains). One might even suggest, that the term terrorism has suffered from inflation, especially from the aftermath of 9/11, and as a result the newer ones are gaining popularity. With such rapidity and prevalence they have spread around contemporary societies.

Here lies the reason for this article. It tries to answer to the need of bringing clarity in understanding the three above mentioned interlinked phenomena: radicalisation, violent extremism, and terrorism, since understanding is the first step on which to build the counter-measures needed tackling the problems.

The angle or paradigm[215] of this article from which the phenomena are looked, is partly from individual's point-of-view, partly from the viewpoint of working life. The emphasis is on preventing someone from the working life of becoming a victim of the radicalisation process: either as a target of maleficent acts, or as the perpetrator. This perspective serves also those interested or obliged in upholding safety and security of an organisation, since looking radicalisation as a problem inside the organisation is often neglected. Also, it is the arena where employers have the authority and responsibility to act: they have the duty of care to their employees, including against radicalisation, violent extremism and terrorist attacks. For example, in Finland the Occupational Safety and Health Act dictates that everyone is entitled to safe work environment. This includes of course freedom from physical threats and violence.

[215] More about scientific paradigm, see for example kestrana (2016). What Is a Scientific Paradigm? *Owlcation.com!* Online. Retrieved from https://owlcation.com/humanities/What-is-a-Scientific-Paradigm

This article does not give any precise guidelines or specific to-do-lists for countering the problem. Rather, it illuminates theoretical aspects that are crucial in understanding limits and possibilities for building counter measurements. The measurements themselves – whatever they might be – are left to ponder by each reader themselves. Further, this article does not, and cannot even try to cover all the aspects of radicalisation, violent extremism or terrorism, e.g. perpetrators' motives, tactics, the concept of martyrdom, the significance of religion, gender issues, or the role of the media etc. The primary aim is to give theoretical tools for preventing working life of becoming a possible victim of radicalisation, violent extremism and related terrorism.

This paper is structured in the following way. First is shortly presented the research field and its complexity. Then, some clarity is brought in the form of defining key concepts, and further explaining the peculiarities of radicalisation, violent extremism and terrorism. Above is followed by presenting the theoretical starting points in understanding radicalisation, violent extremism and terrorism from counter-measurements perspective (a noteworthy distinction between understanding and approving must be clarified. This paper does not in any way admire or approve violent extremism). Then after, emphasis is on the areas in which successful counter-measurements are possible, i.e. where the problem can be tacked, together with suggestions for action alongside with some examples from real life.

1. Countering Radicalisation, Violent Extremism, and terrorism in contemporary working life

1.1. Radicalisation, violent extremism, and terrorism: full of ambiguity

Radicalisation and violent extremism, not to mention terrorist attacks are extremely rare. In fact, the risk of dying from an attack is between dying from a bee sting and lightning strike.[216] Still, many are eager to try to understand the phenomena. Understanding is after all, the nature of science.[217] The urge to understand may also derive from rationality, which has ever since the Enlightenment constantly been reminded to the western man (and woman too). We need to be reasonable, rational, and weigh things up in a logical and considered way.[218] This is especially true in working life. Becoming radical seems irrational for many. Even fewer find reason in involving with violence and terrorism, let alone in individual's willingness to suicide. Perhaps then, there is an epistemic reason that arises from the curiosity about peculiar phenomena?[219] Or, is it just that deviance has always attracted attention?[220]

Whatever the truth is, understanding or explaining the phenomena is hard. Hence, there is a strong dissension on how to

[216] Palmer, I. (2007). Terrorism, Suicide Bombing, Fear and Mental Health. *International Review of Psychiatry*, No. 19(3), pp. 289–296

[217] Der Regt, H. W. and Dieks, D. (2005). *A Contextual Approach to Scientific Understanding*. Synthese, 144, pp. 137–170

[218] Clarke, S. (2006). *From Enlightenment to Risk. Social Theory and Contemporary Society*. Basingstoke: Palgrave McMillan

[219] Kruglanski, A. W. (2009). Fully Committed: Suicide Bombers' Motivation and the Quest for Personal Significance. *Political Psychology*, No. 30(3), pp. 331–357

[220] Greer, C. ed. (2010). *Crime and Media: a Reader*. London: Routledge

explain radicalisation, violent extremism and terrorism – and especially its most extreme manifestations, such as suicidal attacks, i.e. those that attract huge media coverage.[221] Martha Crenshaw, one of the pioneers in terrorism studies, for example, argues that: "explanations are still at an early, and uneven stage. The concept remains imprecise, the facts are not well established. Findings are often based on incompatible datasets, and references to cases or examples do not always fit the stated definitions of the concept. Contradiction, ambiguity, and error are particularly consequential because the overall number of suicide attacks [and other attacks] is quite small."[222] Robert A. Pape, American political scientist known for his work on international security affairs and suicide terrorism, agrees with Crenshaw, and states that "we do not have a good explanation of the growing phenomenon of suicide terrorism."[223] It has also been acknowledged, that no single model can fully explain neither radicalisation and violent extremism nor terrorism. The phenomena are multifactorial, and need often to be considered from an interdisciplinary perspective.[224] An approach that combines e.g. philosophy, anthropology, history, psychiatry, criminology, terrorism, and security studies is very much needed.

Usually, the ambiguity begins to disappear as more explanations are made. However, this seems not be the case when exploring the

[221] Eid, M. ed. (2014). Exchanging Terrorism Oxygen for Media Airwaves: The Age of Terroredia. Hershey, PA: Information Science Reference

[222] Lankford, A. (2010). Do Suicide Terrorists Exhibit Clinically Suicidal Risk Factors? A Review of Initial Evidence and Call for Future Research. *Aggression and Violent Behaviour*, No. 15, pp. 335

[223] Pape, R. A. (2003). The Strategic Logic of Suicidal Terrorism. *The American Political Science Review*, No. 97(3), pp. 343

[224] Post, J. M. et al. (2009). The Psychology of Suicide Terrorism. *Psychiatry*, No. 72(1), pp. 13–31

phenomena of radicalisation, violent extremism and terrorism. Internationally recognised leading expert on terrorism and low intensity conflict, Andrew Silke wrote already in the beginning of the millennia about terrorism related research in the following way: "[it] exists on a diet of fast-food research: quick, cheap, ready-to-hand and nutritionally dubious".[225] The situation has not changed much, since the appetite for related research is huge. Not only the public wants to read about terrorism, but the urge to understand derives from authorities, especially law enforcement agencies, and also others, including businesses. Especially sought are answers for countering the problem.

The problem however remains. Despite all the research, or perhaps because of it, even general agreements on the basic definitions and key concepts of radicalisation, violent extremism and terrorism are difficult to achieve. As a result, an all-embracing, and in-depth answers covering all seems elusive, too.

1.2. Bringing clarity and coherence

Every incident of either radicalisation, violent extremism, or act of terrorism are events, which cannot be fully understood outside their unique historical, cultural, and political context. However, a broader explanatory level of each phenomena is nevertheless acknowledged. Furthermore, for any meaningful analysis one needs to define terms and concepts, so that the audience has a clear view on what the author means. Thus, the three phenomena addressed in this paper are presented shortly below.

[225] Silke, A. (2008). Research on Terrorism: A review of the impact of 9/11 and the global war on terrorism. *Terrorism Informatics: Knowledge Management and Data Mining for Homeland Security, Integrated Series in Information Systems*, Vol 18, eds. H. Chen, E. Reid, J. Sinai, A. Silke, and B. Ganor. New York: Springer

Radicalisation refers to becoming radical, i.e. transforming into a nonconformist and/or rebellious, for example, someone who thinks that there should be great or extreme social, political, or economical changes. Becoming radical is always subjective, since it needs to be compared to the general views and values. It must be noted, that being radical is not necessarily a negative term. Radicals are actually needed in societies: without them, everything stays static. Often progress is because of radicals, people such as Steven Jobs, Martin Luther King, Gandhi, Copernicus…[226]

One might argue that radicalisation is, however, a precondition for violent extremism, the second phenomena addressed in this paper. The distinction between radicalisation, i.e. a person with radical ideas and a violent extremist lies in the violence. Thus, in the willingness of using violence in achieving radical goals. Often, violent extremism is presented as something that follows radicalisation, thus as a process where radicalisation is the pre-phase. The idea of process is presented more in details further below in this article. The critical thing, however, is the distinction between radical ideas, how disrupting they may be, and with willingness for violence. Violence (or the threat of it) is precisely the key in making the distinction. Thus, there is seldom anything positive in violent extremism.

Terrorism is one of the most contested terms. One man's terrorist is another's freedom fighter, as *ye olde* saying goes. For example, American Sociologist Axel P. Schmid analysed already in 1984 101 different definitions of terrorism, that had 22 different

[226] Fitzgerald A. (2014). Being labeled a 'radical' is meant to be an insult. History tells us otherwise. The Guardian. Jan 20. Retrieved from https://www.theguardian.com/commentisfree/2014/jan/20/we-need-radicals-for-social-change

defining aspects. However, he found no single definitions included all the aspects.[227]

In this article, terrorism can be understood as the end-result of violent extremism. It is the ultimate manifestation of the radicalisation process. This view is close to, for example, terrorism expert Brian Jenkins' point of view: it is the nature of the acts that define terrorism, not the identity of the perpetrators, or their motives.[228]

Therefore, pivotal for understanding the differences of the three phenomena, is that terrorism is beyond all, a tactic. It is a set of tools for a particular behaviour, whether it is bombing, armed attacks, letter bombs, highjacking an aeroplane or train, taking hostages, assaulting people generally or specifically targeting, for example, associations. Terrorism is all about fear: creating and using it for a purpose. In terrorism, there is always a larger audience than the imminent people affected by it. Thus, many say that there cannot be terrorism without publicity.

Another difference between radical, violent extremism and terrorism is that arguably you do not have to be radical and/or extreme to be a terrorist.[229] As explained above, radicalism and extremism were always in relation with existing normative rules. Thus, for example, someone who is born and raised in a culture of hate and violence, where terrorist acts are seen as accepted and

[227] Piper, G. (2002). Was ist Internationaler Terrorismus? Begriffsdiskussion, Geschichte, Organisationen und Finanzen eines Gespenstes. Friedenspolitischer Ratschlag. Retrieved from http://www.uni-kassel.de/fb5/frieden/themen/Terrorismus/piper2.html

[228] Jenkins, Brian M. (1982). Statements about Terrorism. *The Annals of the American Academy of Political and Social Science*, 463 (Sep.), pp. 11–23

[229] Borum, R. (2011). Radicalization into Violent Extremism I: A Review of Social Science Theories. *Journal of Strategic Security*, No. 4(4), pp. 7–36

justified reactions, for example, against an entity considered as an unjust oppressor, then the person is not radical, since his or her views are in the mainstream. Since, radical and/or extreme is atypical from conventional norms, for those to whom terrorism is ordinary, radical or extreme views are not needed. This is the unfortunate state of affairs in many parts of the world, when certain societies, part of societies, and/or (sub)cultures for whatever reason see terrorism somewhat normal.

2. What is needed for successful counter–measurements?

2.1. First to understand: it is a process!

The most critical thing in understanding how radicalisation and violent extremism can be tackled comes perhaps from combining three different assumptions. The first is acknowledging that there exists a process of radicalisation into violent extremism and all the way to terrorism. However, the process is a theoretical starting point, a precondition for treating the subject, not necessarily the whole truth. Without acknowledging the idea of a radicalisation process, for example, attempts to intervene the phenomena would be totally different than, for example, if radicalisation is a necessity, act of God, or the result of genotype.

The problem with processes is that usually the outcome is known. For example, in a process which has as an end a suicide attack, the ending can be relatively easily defined: it is the moment when someone blew himself up. However, identifying the so-called tipping point, let alone the starting point is much more complicated, often completely speculative. Nevertheless, it has been acknowledged that the process of radicalisation is rather months than weeks, although some have been radicalised even in days to the point of committing serious atrocities such as suicide bombings.

The process can be pictured as climbing ladders, pyramid, or even as simplistic as an arrow.[230] Similarly, the visualisation can stress different aspects of the process, from the process itself to the so-called terrorist mind-set. Below are examples of the process itself (Figure 1), and the possible changes mind-set (Figure 2).

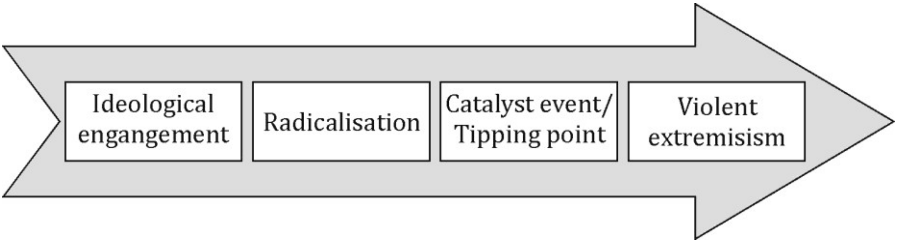


Figure 1. **Illustration of the Radicalisation Process**

The first figure illustrates the process from mere ideological engagement, e.g. supporting mentally the cause or ideology, to more severe radicalisation, i.e. when the ideas start to manifest as acts. [231] The acts in this stage are, for example, writings online, preaching and campaigning to friends and family or other communities, so not necessarily anything illegal. The latter stages of the process are the so-called tipping point, i.e. the point at which the build-up of minor incidents reaches an unbearable level, causing someone to act in a way that they had formerly resisted. This point can lead into violence.

[230] Muro, D. (2016). What Does Radicalisation Look Like? Four visualisations of socialisation into violent extremism. *Notes internacionals CIDOB*, 163, pp. 1–5, inspiration for the figures 1–3. 15

[231] Schmid, Alex P. (2013). Radicalisation, De-Radicalisation, Counter-Radicalisation: A Conceptual Discussion and Literature Review. *ICCT Research Paper*

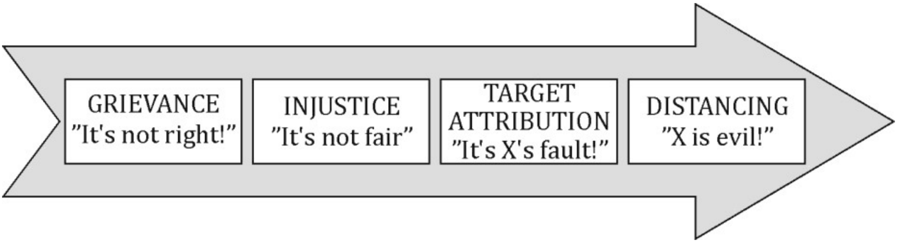


Figure 2. **Illustration of the Process of the Maturation of the so-called Terrorist Mind-set**

The second figure of the process is related more into the changes in the mind-set.[232] First, is the awakening to wrongs of the world: something is not right and it is not fair. The next phase is to find a culprit, someone whose fault it is, or someone who can be blamed for. The last phase is related with becoming in terms with possible justifications for harmful action and violence, thus distancing oneself from the victim by derogating and demonising the target of violent acts.

Both arrows point straight forward to one direction only, although in real life there are back and forth movements. Similarly, someone can skip one phase and move to the next. Also, it must be noted that the time scale varies substantially: the process is not linear in the sense that the duration of phases is not equal. For example, the grievance phase (Figure 2) can be substantially longer than the distancing, or then maybe not: it depends always on the individual and his or her course of life.

Using the wording “have been radicalised” in the couple paragraphs above is done deliberately. The reason for this is that related to the concept of a process, many researchers, for example,

[232] An adaptation from Borum, R. (2003). Understanding the Terrorist Mindset. *FBI Law Enforcement Bulletin*, No. 72(7), pp. 7–10

famous terrorism expert Ariel Merari, has emphasised the role of the organisations (and even states). Merari has stated the following: "I don't know of a single case in which an individual decided on his or her own to carry out a suicidal attack. In all cases – it certainly is true in Lebanon and Israel and Sri Lanka and the Kurdish case – it was an organization that picked the people for the mission, trained them, decided on the target, chose a time, arranged logistics and sent them."[233] Thus, besides providing for material and logistical needs, the organisations have a crucial role in making radicalised people into violent extremists and terrorists: they assure and strengthen the commitment of the candidates ultimately into actually blowing themselves (and the targets) up.

Above can been seen also in the visualisation below (Figure 3), yet again emphasising the importance of the process.[234] Here, the logic is from sympathiser to the violent extremist, and the width of the building blocks represents the number of persons in each category. The critical thing to understand is that behind every extremist is a vast number of people who act as enablers. This is true even when speaking about so-called lone wolf terrorism, perhaps with the exception of extreme cases, such as the Unabomber, for example.[235]

In the following pyramid are presented the different groups of people that enable radicalisation, violent extremism and terrorism all playing their roles.

[233] Vedantam, S. (2001). Peer Pressure Spurs Terrorists, Psychologists Say; Attackers Unlike Usual Suicide Bombers. *The Washington Post*, October 16, p. A16

[234] An adaptation of a model presented in McCauley and Moskalenko, 2008. Also presented in "Mechanisms of Political Radicalization: Pathways Toward Terrorism", *Terrorism and Political Violence*, 20:3, (2008), pp. 415–433

[235] Spaaij, R. (2010). The Enigma of Lone Wolf Terrorism: An Assessment. *Studies in Conflict & Terrorism*, NO. 33(9), pp. 854–870

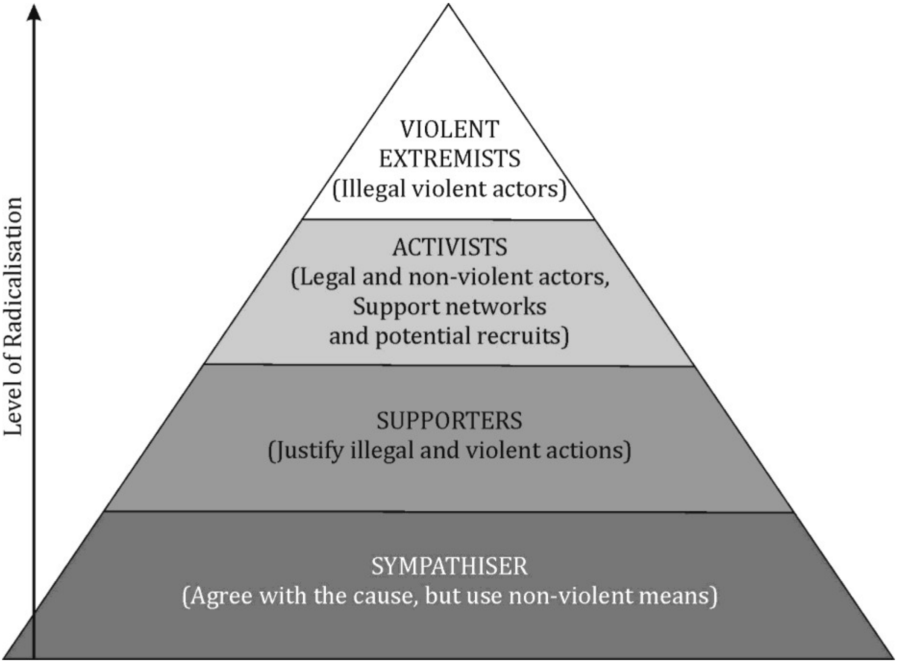

Level of Radicalisation
VIOLENT EXTREMISTS (Illegal violent actors)
ACTIVISTS (Legal and non-violent actors, Support networks and potential recruits)
SUPPORTERS (Justify illegal and violent actions)
SYMPATHISER (Agree with the cause, but use non-violent means)

Figure 3. **The Pyramid Model of Radicalisation**

At the bottom are those who sympathise and support the cause. They are essential, since they give the meaning to the action: they are both the larger suffering community on behalf of whom the acts are committed but also the audience that resonate reasoning for further acts. Without them, the sacrifices of the perpetrator on behalf of the paramount cause would be all in vain. They also help in the mental processes of becoming radical, since the share number makes the cause larger than, for example, personal vendetta. The group just below the violent extremists, i.e. those who commit the illegal violent acts, is the activists. They often support and supply the extreme ones with logistics and material for conducting the violence (bombs, guns, ammunition etc.).

Following the first crucial starting point in understanding radicalisation, violent extremism and terrorism, let us move into the suitable theories to follow when tackling the problems. These are Routine Activity Theory (RAT) and Situational Crime Prevention (SCP).

2.2. Theories to Follow: Routine Activity Theory and Situational Crime Prevention

Moving from the process into the next topic, and closer to the actual counter-measurements of radicalisation, violent extremism, and terrorism, two theories need to be introduced: Routine Activity Theory (RAT) and Situational Crime Prevention (SCP).

The two theories have lots of shared points, because they have common roots. One might say that the latter is more of a practical outcome of the first, and that often it is unnecessary to even distinct one from another. The focus of the two theories is in the idea that the most efficient way of reducing harm can be achieved by altering situations, and that those situations often are results of mundane life itself, in the routines in which people interact with each other's. The interest is thus not in offender's personal characters or motives for purely their sake. Rather, the stress is on increasing the effort of committing crime, increasing the risk of getting caught, reducing the reward, reducing provocations and reducing excuses. Following the above logic, for example, the "father" of SCP, Ronald V. Clarke categorised crime prevention approaches into the amount of surveillance (e.g. CCTV, access control…), target hardening measures (e.g. physical barriers, locks, anti-robbery screens, tamper-proof packaging…), and environmental management (e.g. design of premises, lightning, use of music…).[236]

[236] Clarke, R. V. (1983). Situational Crime Prevention: Its Theoretical Basis and Practical Scope. *Crime and Justice: An Annual Review of Research*, NO. 4, 225–256

Critical for the understanding is to know that in any crime, there are two things that need to be present: a motivated offender and a suitable victim. Also important is that a third – so-called capable guardian – is missing. Only then a crime can happen. This is illustrated in the figure below (Figure 4).[237]

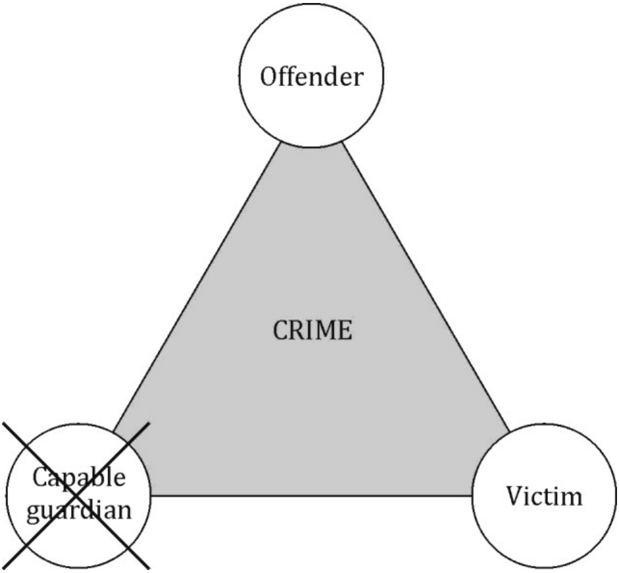


Figure 4. **The Crime Triangle**

In the context of radicalisation, violent extremism and terrorism, the motivated offender can be either the violent extremist or terrorist, but also they themselves can be victims of the radicalisation process. Often, a suicide attacker is a victim too. In these cases, the offender is someone who is trying to recruit suitable candidates or persuade radicals into more sinister doings. The capable guardian can be anyone, or anything, that prevents the

[237] Felson, M. and Boba, R. (2010). *Crime and Everyday Life*, 4th ed. London: Sage

interactions between the motivated offender and suitable victim. In everyday crime prevention, police or security guard is an obvious choice. However, the role of unofficial policing, e.g. from lay men or family members cannot be ignored. For example, even grandmothers can be an excellent crime stoppers.

Since the victim in radicalisation cases meant two things, i.e. the radicalised person herself or the person's target of malicious acts, the capable guardian in radicalisation context means various sets of actors, too. The first set is those preventing the acts themselves when the radicalisation process is at its final phases, ultimately the violent aggression. The second are those who target more the radicalised person from becoming violent extremist, and of course then preventing the violent acts. When thinking the possible capable guardians, law enforcement is of course one obvious, but in a working life environment, a capable guardian can be a colleague, supervisor, security personnel, but also janitor, concierge, or IT-technician – actually anyone who can intervene the interaction between the offender and victim. The theories does not imply directly what kind of action is the interventions. The Crime Triangle (see Fig. 4) for example presents the conditions for crime, no more. The actual doings are thus presented in the next paragraph where the theories are put in action.

3. Putting Theories into Practice[238]

When putting the theories – i.e. the presupposition of radicalisation being a process, Routine Activity Theory (RAT), and Situational Crime Prevention (SCP) – into practice it must be

[238] This section's knowledge base is from a EU funded research entitled RAVET – Radikalisaation ja Väkivaltaisen Ektremismin Torjuntamalli korkeakouluille, in which the author had the privilege of being the project manager and do research

stressed that, since the three phenomena – radicalisation, violent extremism and terrorism – have fundamental differences presented in the previous paragraphs, the counter-measures of cannot be alike. For example, since the be-all and end-all of terrorism is more than anything a tactic full of action, the counter-measures are obviously different from cooling down someone's radical ideology. Thus, rather than presenting counter-measurements on an anecdotal level, it is more advantageous perhaps to concentrate on the question where does lie the arena for possible counter-measurements in contemporary working life.

3.1. The Aim: Intervene the Process

If we take the theories presented above as the starting points when thinking of tackling the phenomena, several implications can be made. First is that the most fruitful would be to stop or intervene the radicalisation process. This seems to be obvious, but is in real life very complicated. For example, since the beginning the process is often in obscurity, as explained earlier, it is very hard to determine when action is needed. Thus, perhaps more appropriate is to concentrate on strengthening structures that enable the process turning grave. In this, the RAT and SCP help to allocate the resources and focus the activities. Since, RAT and SCP both stress the interaction between humans (the offender and victim) as well as emphasises that crime (in this case the radicalisation process) seldom happens outside the everyday life, the counter-measurements need to be something that is present in the same environment with the offender and victim, as well as something that somehow changes the perpetrator's undesired behaviour.

3.2. The Arenas

In contemporary working environments there are few arenas for the counter-measurements. The starting point would be recruitment. What could be more efficient than preventing the possible radical elements of becoming a part of the working life to begin with? But what if employers radicalise after being hired? Can employers control their lives to the point they are fully aware of what is going on in their minds? In small businesses in tight communities, for example, a family run small shop this might be possible, or then maybe not. Working life is indeed important for many, but it is seldom the whole life: people get influences from outside working life, too. Furthermore, what are the rights of the employers to control the employees? Thus, the arenas for counter-measures must be first and foremost areas where employers have the right to act. One of these is, of course, the infrastructure in which the business is run.

Making changes in the infrastructure of any working life can highly affect, for example, the efficacy of work, work conditions, ambience, how the work is done etc. Thus, it is conclusive that making changes would affect radicalisation process, too.

Two different domains of business' infrastructure must be made. First is the premises, and the second is the so-called IT-infrastructure, both vital in today's world – the latter more and more. When thinking the premises or IT-infra, tackling radicalisation, violent extremism and terrorism threats coming from outside the organisation, especially imminent threats, is no different than securing the everyday business overall. For example, physical security against any bomb attacks or cybersecurity against malwares needs to be taken into account. What is perhaps different, is the need to be prepared for tackling radicalisation inside the organisation. This means that not only outsiders are kept away from unwanted premises, but also that the organisation has a good picture of who is using the premises and for what purpose. For example, the use of meeting rooms etc. must be well justified and also documented.

Since a lot of radicalisation happens online, information technology (IT) infrastructure is critical. Thus, when legally possible, an organisation might, for example, restrict employees' access to only work related webpages, block the use of social media etc. However, more pertinent is that there are strict and clear guidelines on the use of IT-infra: for example, what is allowed to do, what material can be saved into workplace's server. The question is not about what is legal and what is illegal. For example, whilst beheading videos or rantings of radical demagogues are not necessarily illegal *per se*, they are surely against the values of (many) companies. Thus, it should be clear, whether an employee is allowed to store this kind of questionable material on employers' server of cloud service.

Also things to take into account are software and hardware. For example, such a mundane machine as a copy machine and/or printer can be used in the radicalisation process. Undesirable material, e.g. propaganda flyers, posters etc. might be reproduced using employers' resources. Thus the goal would be preventing working environment from being supportive of the radicalisation process. To sum up, it means that the resources that are available for better performance at work are not used in doings that are dubious, against employers' values, or illegal.

3.3. The Counter–measures

The second area where radicalisation process can be addressed is common educational activities. The contemporary working life is investing more and more in employers' training and education. Here too lies an arena for countering radicalisation process. The employers do not have to learn deeply about radicalisation itself, but rather to adopt values that do not promote radicalisation. Pivotal to all is, that everyone is aware of the different legislation, rules, guidelines and best practices that guide the working life. All above reflect the values a company wants to follow. Also important is the example of others, and especially superiors. Thus, the management needs to be committed to the values.

Ideally, tackling radicalisation does not need to happen in a void, but rather when dealing with normal working life processes. Thus, for example, simple and unambiguous user guides for the use of IT services and premises, what are organisation's general do's and don'ts, directions on what to do when anomalies are spotted or when anything give rise to concern – these all serve also as the base of countermeasures for enabling the radicalisation process. Naturally, one key element is the mechanism that allows people to let know about their concerns, whether there is a specific process for that or a simple email to superiors.

In order to keep the countermeasures in proportion, i.e. not reacting too harshly, there should always be an evaluation mechanism in place. Whether it is a simple check list or more elaborated risk analysis model, the indications that leads to suspected radicalisation process should be evaluated. The evaluation then guides how to tackle the problem in concrete level, e.g. should those who are responsible for the security contact law enforcement.

Conclusions

Radicalisation, violent extremism and terrorism are a recognised problem in contemporary working life. However, they can be dealt with. The answer lies in understanding the basic logics of what these phenomena are, but also what theories would be beneficial when tackling the problem. Too often, counter-measurements are done without a solid theoretical base, whether it is preventing crime or more sinister phenomena. Sir Francis Bacon's famous statement, knowledge is power ("Nam et ipsa scientia potestas est")[239], is still very relevant. Hopefully, this article has activated thoughts that can be put into further practical use. The practices themselves then depend, of course, on the organisations' particularities and needs.

References

Borum R. (2003). Understanding the Terrorist Mindset, *FBI Law Enforcement Bulletin*, No. 72(7), pp. 7–10

Borum R. (2011). Radicalization into Violent Extremism I: A Review of Social Science Theories. *Journal of Strategic Security*, No. 4(4), pp. 7–36.

Clarke R. V. (1983). Situational Crime Prevention: Its Theoretical Basis and Practical Scope. *Crime and Justice: An Annual Review of Research*, No. 4, pp. 225–256

Clarke S. (2006). *From Enlightenment to Risk*. *Social Theory and Contemporary Society*. Basingstoke: Palgrave McMillan

Der Regt H. W. and Dieks D. (2005). A Contextual Approach to Scientific Understanding. *Synthese*, 144, pp. 137–170

Eid M. ed. (2014). Exchanging Terrorism Oxygen for Media Airwaves: The Age of Terroredia. Hershey, PA: *Information Science Reference*

Felson M. and Boba R. (2010). *Crime and Everyday Life*, 4th Ed. London: Sage

Fitzgerald A. (2014). Being labeled a 'radical' is meant to be an insult. History tells us otherwise. The Guardian. Jan 20, 2014. Retrieved from https://www.theguardian.com/commentisfree/2014/jan/20/we-need-radicals-for-social-change

Greer C. ed. (2010*). Crime and Media: a Reader*. London: Routledge

Jenkins B. M. (1982). Statements about Terrorism. *The Annals of the American Academy of Political and Social Science*, No. 463(Sep.), pp. 11–23

[239] Knowles E. (ed.) (2004). *Oxford Dictionary of Quotations*, 6th Ed. Oxford and New York: Oxford University Press

Knowles E. (ed.) (2004). *Oxford Dictionary of Quotations*, 6th Ed. Oxford and New York: Oxford University Press

Kruglanski A. W. (2009). Fully Committed: Suicide Bombers' Motivation and the Quest for Personal Significance. *Political Psychology*, No. 30(3), pp. 331–357

Lankford A. (2010). Do Suicide Terrorists Exhibit Clinically Suicidal Risk Factors? A Review of Initial Evidence and Call for Future Research. *Aggression and Violent Behaviour*, No. 15, pp. 334–340

McCauley C. and Moskalenko S. (2008). Mechanisms of Political Radicalization: Pathways Toward Terrorism, *Terrorism and Political Violence*, No. 20(3), pp. 415–433

Muro D. (2016). What Does Radicalisation Look Like? Four visualisations of socialisation into violent extremism. *Notes internacionals CIDOB*, No. 163, pp. 1–5

Palmer I. (2007). Terrorism, Suicide Bombing, Fear and Mental Health. *International Review of Psychiatry*, No. 19(3), pp. 289–296

Pape R. A. (2003). The Strategic Logic of Suicidal Terrorism. *The American Political Science Review*, No. 97(3), pp. 343–361

Piper G. (2002). Was ist Internationaler Terrorismus? – Begriffsdiskussion, Geschichte, Organisationen und Finanzen eines Gespenstes. Friedenspolitischer Ratschlag. Retrieved from http://www.uni-kassel.de/fb5/frieden/themen/Terrorismus/piper2.html

Post J. M. et al. (2009). The Psychology of Suicide Terrorism. *Psychiatry*, No. 72(1), pp. 13–31

Schmid Alex P. (2013). Radicalisation, De-Radicalisation, Counter-Radicalisation: A Conceptual Discussion and Literature Review. *ICCT Research Paper*

Silke A. (2008). Research on Terrorism: A review of the impact of 9/11 and the global war on terrorism. Terrorism Informatics: Knowledge Management and Data Mining for Homeland Security, Integrated Series in Information Systems, Vol 18, eds. H. Chen, E. Reid, J. Sinai, A. Silke, and B. Ganor. New York: Springer

Spaaij R. (2010). The Enigma of Lone Wolf Terrorism: An Assessment. *Studies in Conflict & Terrorism*, No. 33(9), pp. 854–870

Vedantam S. (2001). Peer Pressure Spurs Terrorists, Psychologists Say; Attackers Unlike Usual Suicide Bombers. *The Washington Post*, October 16, p. A16

About the Author

Tuomas Tammilehto, *M.Soc.Sci.* (political history), MA Criminology
Tuomas Tammilehto is a social scientist (M.Soc.Sci. from University of Helsinki, major in Political History) and a criminologist (MA in Criminology from City University London). His main areas of expertise and interests are criminology,

radicalisation, policing, knowledge management, terrorism and contemporary history.

Tuomas has spent most of his work life in academia at the Helsinki Collegium for Advanced Studies (University of Helsinki) and at Laurea University of Applied Sciences teaching, carrying out research, and managing security related international research projects.

Tuomas is originally from Helsinki but have lived also in Tübingen (GER), Paris and London. He has been characterised by his students and colleagues as truly international, well networked, widely civilised and easily approachable.

EU INTEGRATED APPROACH TO RESPOND CONFLICTS AND CRISIS

Petteri Taitto
Kirsi Hyttinen

Introduction

European Union is a regional security actor, as it has been founded to safeguard the security and prevent war in Europe after the Second World War. The EU has evolved to security union and one of the founding documents along the Treaty of the Union is the EU Global Strategy, which sets the goals, priorities and ambitions when placing EU to the global scene and world order. One of the Global Strategy priorities is EU Integrated Approach to respond conflicts and crisis, which addresses all dimensions and stages of a conflict. Integrated Approach sets a particular emphasis on early warning and early action before a crisis erupts.[240]

The Integrated Approach outlines how to ensure rapid and effective crisis response, from building greater synergies between the different EU institutions, how to conduct Common Security and Defence Policy (CSDP) and crisis management in line with other EU capacity-building missions and operations. All mechanisms are subsequent to the political processes, including trade and even sanctions policies of the EU.[241]

[240] A Global Strategy for the European Union. (2016). Retrieved from https://europa.eu/globalstrategy/en

[241] An Integrated Approach to external conflicts and crisis. 7 June 2017. European External Action Service 10054/2017

This article gives an overview on how EU manages crisis globally, in the various phases of crisis and using various EU instruments. The article begins by presenting EU Global Strategy and its relation to security. After that the EU Integrated Approach to respond conflicts and crisis is presented more in detail, and finally few examples of the successes of Integrated Approach are given.

The article stresses the importance of active strategic communication as strategic communication is also an important part of the EU public diplomacy. Likewise, general awareness of EU security structures in both EU institutions and in the EU Member States is important to make the union even more functional in the future

1. Value based security strategy

The EU is constituting its activities by the values on which it is founded, and its greatest achievement is the peace between Member States after the Second World War. "The Union's aim is to promote peace, its values and the well-being of its peoples. The values of respect for human dignity, freedom, democracy, equality, the rule of law and respect for human rights, including the rights of persons belonging to minorities. (Treaty of the EU, Art 2 and 3). Security in the Union and in its neighbourhood is therefore one of the cornerstones for the existence of the EU. All security norms and policies are based on the values of the Union, values that like-minded Member States have agreed to be the glue of the Union.

In the current changing security environment, values are the only prevailing thing. Europe is facing a great range of complex and dynamic threats and challenges, both internally and externally. The new security environment requires a strong European Union, able to promote peace and guarantee the security of its Member States and citizens, as agreed in the Treaty. Traditional way of managing the threat is either to protect from it, or make an effort to have an influence to its sources[242], and according to the EU Global Strategy the European Union is enhancing its external security by responding to external conflicts and crises, building the capacities of partners and protecting the Union and its citizens outside of the Union borders.[243]

First of the strategic priorities mentioned in the Global Strategy, responding to conflicts and crisis, has been also the core of the Common Security and Defence Policy (CSDP) of the Union. The CSDP provides the Union with an operational capacity to deploy both civilian missions and military operations. The range of tasks is set out in the EU Treaty: humanitarian and rescue tasks; conflict prevention and peace-keeping tasks; tasks of combat forces in crisis management, including peace-making; joint disarmament operations; military advice and assistance tasks; post-conflict stabilisation tasks.

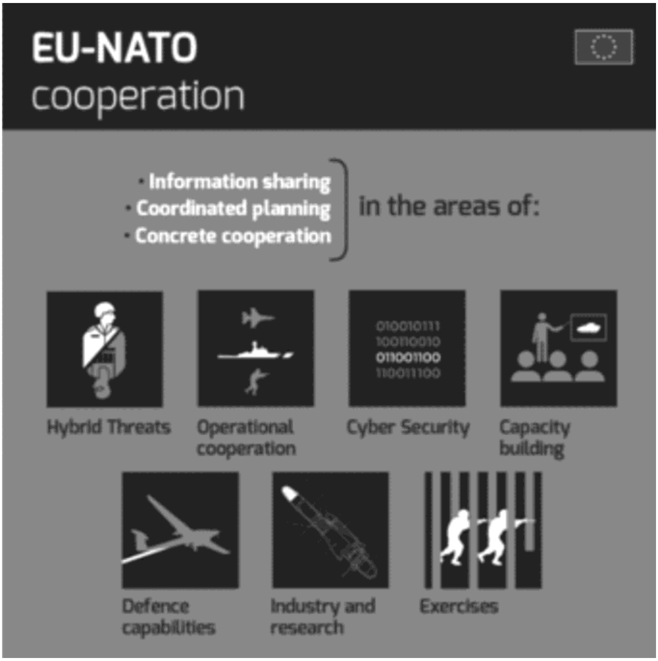
The second aspect in the Global Strategy is building capacities of its partners. The Union has developed a special relationship with neighbouring countries, aiming to establish an area of prosperity and good neighbourliness, founded on the values of the Union and characterised by close and peaceful relations based on cooperation. This strategic goal is fully in line with the Treaty article 8 that stipulates that the Union may conclude specific agreements with the countries concerned. These agreements may contain reciprocal rights and obligations as well as the possibility of undertaking activities jointly.

[242] Buzan B. (1983). *People, States & Fear*. Routledge

[243] A Global Strategy for the European Union (2016). Retrieved from https://europa.eu/globalstrategy/en

The partnerships with neighbouring countries foster the sustainable development in the neighborhoods. The European Neighborhood Policy (ENP) was launched in 2004 based on a Communication entitled “Wider Europe – Neighbourhood” adopted by the European Commission one year earlier. The Policy was set as a framework to govern the EU's relations with 16 of the EU's Eastern and Southern Neighbours in order to achieve the closest possible political association and the greatest possible degree of economic integration.

EU has also numerous partnerships with international organisations, such as the United Nations, the NATO and the International Organization of Migration, IOM. The partnership with IOM responds to the urgent protection needs that EU has been facing in the last few years. Likewise, the partnership with NATO has increased and deepened recently: in 2016, 42 joint actions were announced and a year after 34 more was added to the list.



Picture 1. **EU-Nato cooperation**[244]

The last priority is to protect EU and its citizens. This aspect is broad, containing a large number of actions, some to mention are Counter Terrorism and EU defence. Counter Terrorism as a matter of national security is mainly a Member States competence, whereas European External Action Service, EEAS, focuses on the external dimension of Counter Terrorism in close coordination with the Member States in the Council Working Groups and with other EU bodies. EEAS' role is to coordinate Counter Terrorism external outreach and capacity building assistance to third countries by EU and its Member States, to ensure coherence and efficiency.

[244] European External Action Service (2018). Factsheet. Retrieved from https://eeas.europa.eu

The EU Global Strategy is also to provide strategic guidance for Member States and EU officials on how to develop EU security and defence priorities in terms of geography and in terms of the range of activities envisaged. It also brings clarity on EU's civilian and military Level of Ambition and matches security priorities with policies. According to the Global Strategy, the EU remains committed to strengthen security and defence. To this end, the EU is enhancing its ability to act as a security provider, as well as its global strategic role and its capacity to act autonomously when and where necessary and with partners wherever possible.[245]

The EU work on security and defence has not just focused on CSDP Missions and Operations. Lately the EU has established a Coordinated Annual Review of national defence budgets, and the European Commission has set up a European Defence Fund. Both of the initiatives are to commit common resources to invest in defence and to help Member States spend better by spending together. In addition, 25 Member States have launched a Permanent Structured Cooperation (PESCO) on defence: a historic move to facilitate cooperation between armed forces, and to fill some crucial gaps in capabilities, and make EU defence spending much more efficient.

2. EU's multidimensional and coordinated response – the integrated approach

When EU's security interests or the security of the EU or its citizens, are threatened, the EU will act by all available means to protect its security and respond to the causes of instability. EU has developed common policies for different areas of security to better

[245] Council conclusions on Security and Defence in the context of the EU Global Strategy 9178/17 17 May 2017

respond to emerging threats. Such policies as Disarmament, Non-Proliferation, and Arms Export Control policies, Fight against piracy, Maritime Security and Common Security and Defence Policy are all mechanisms, that Member States are jointly willing to promote in order to enhance internal and external dimensions of security. In addition European External Action Service, EEAS, has developed a specific Crisis Response Mechanism to respond more rapidly to a crisis that EU may encounter.

Furthermore, when the EU is facing a sudden crisis or an emergency that can be caused by deterioration of security, political or economic situation in a country or region, a specific Crisis Response Mechanism is launched in the structures of the EEAS. The common nominator is that the event or development can have an impact on the security interests or the security of the EU and its citizens. The Crisis Response Mechanism functions in the spirit of the Integrated Approach as it should envisage the use of all available resources in a coordinated way.[246]

The activation of the Crisis Response Mechanism takes place in the Crisis Meeting, where EEAS and Commission senior managers assess the short-term effect and decide which course of action is necessary. The possibilities are Immediate Action, Activation of Crisis Cell, and convening the Crisis Platform. In some cases a specific Task Force, chaired by competent geographic desk of EEAS.

A description and vision how the EU should improve its capabilities to respond to external crisis and conflicts was presented in the EU Comprehensive Approach to external crisis and conflicts. One of the founding principles in this document was the shared analysis and common vision across the instruments on how to best respond to crisis. It aims to mobilise and synchronise the use of a

[246] Serrano P. (2017). EEAS Crisis Response Mechanism*. CSDP Handbook*. ESDC

wide range of the EU instruments, like political action, sanctions, developmental aid, humanitarian aid and Common Security and Defence Policy (CSDP) actions. The Comprehensive Approach focused on conflict prevention and emphasizes that internal and external action should work closely together and commit always in planning to find the long term solution.[247]

The Comprehensive Approach was followed by the EU Integrated Approach to respond to conflicts and crisis, and it was first introduced in the Global Strategy. The Integrated Approach is more 'vertical' than the Comprehensive Approach as it aims at placing various components of the EU response under a single authority, whereas the CA was more 'horizontal', focusing on the use of multiple EU instruments simultaneously.[248]

The Integrated Approach streamlines the Comprehensive Approach by addressing the phases of the conflict and describing the EU's approach to each of these phases. The Integrated Approach operationalises further the coordination and complementarity of tools and policies. Doing this will create more clarity on the process and enable a more strategic use of the available tools and policies. In this way, the EU together with Member States can be more effective in preventing and responding to external conflicts and crises.[249]

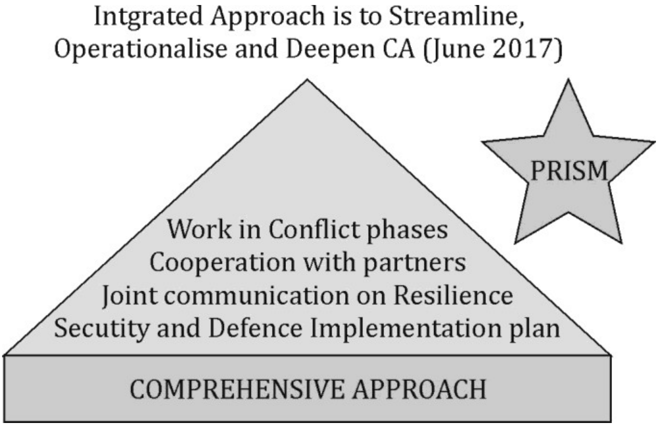
The Integrated Approach is not only a single document, but it can be seen also as a guiding policy for other actions that take forward the Global Strategy security dimension. Other documents are complementary to the Integrated Approach, some to mention

[247] EU Comprehensive Approach to external conflict and crisis. Joint Communication, 11 December 2013

[248] Tardy T. (2017). The EU: from comprehensive vision to integrated action. EUISS Brief Issue 5

[249] Ibid

are the Joint Communication on Resilience and Security and Defence Implementation Plan. In particular, the Joint Communication on Resilience will highlight the relevance of investing in upstream conflict prevention, crisis response and conflict resolution. There are also important areas of read-across with the Security and Defence Implementation Plan, including maximising the potential of the Common Security and Defence Policy as part of a wider EU Integrated Approach to conflicts and crises.[250]


Intgrated Approach is to Streamline,
Operationalise and Deepen CA (June 2017)
PRISM
Work in Conflict phases
Cooperation with partners
Joint communication on Resilience
Secutity and Defence Implementation plan
COMPREHENSIVE APPROACH

Picture 2. **Integrated Approach operationalization**

EU builds its Integrated Approach to the broad conflict cycle, including ‘conflict analysis and prevention’, ‘conflict management’, and ‘post-conflict stabilisation’. When a crisis or conflict breaks out with a potential impact on ‘the security of the Union’, the Integrated Approach highlights a politically and operationally coherent EU response based on a shared analysis. The conflict management is

[250] An Integrated Approach to external conflicts and crisis. 7 June 2017. European External Action Service 10054/2017

bringing together and connecting all EU levels (civil and military, CSDP and EU Delegations, EEAS Crisis Response Mechanism and Commission services, (previously mentioned development and humanitarian aspects, etc.). In the post-conflict stabilization phase, the Integrated Approach is to ensure that transition between EU crisis management and local authorities factually takes place. A coherent stabilisation policy contributes to conflict prevention and thus closes the conflict cycle.[251]

EU's engagement to any crisis is connecting security and development, and EU Global Strategy stresses that development cooperation is an important part of EU external security dimension. It is managed by Directorate–General for International Cooperation and Development, DEVCO, which defines the EU's development policy and implements developmental projects and programmes in the areas where EU has an interest and responsibility to act.[252]

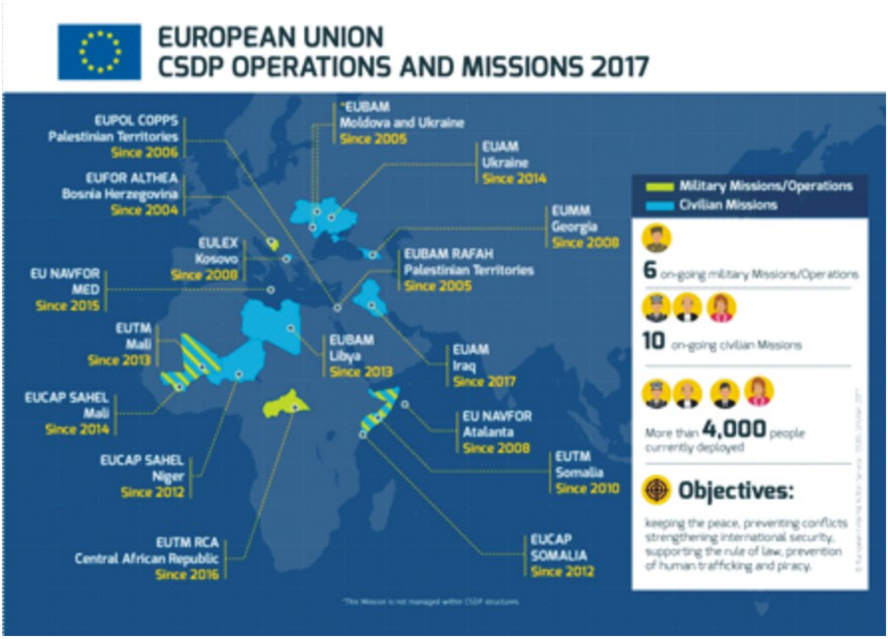
Humanitarian response is one way to alleviate human suffering, but unlike other instruments, it is not politically connected and conditional, as development cooperation. Humanitarian response is driven by humanitarian principles: humanity, neutrality, impartiality and independence – and hence it is called that it is part of EU response but not an integral part of Integrated Approach to respond to crisis.

CSDP missions and operations are a unique tool for direct action, rapidly and in less permissive environments if need be, to manage and help resolve a conflict or crisis. This is normally done at the request of the country to which assistance is being provided and always in full respect of international law. EU decisions to deploy a

[251] Tardy T. (2017). The EU: from comprehensive vision to integrated action. *EUISS Brief,* Issue 5

[252] Boutillier C. (2017). The Security and Development Nexus. *CSDP Handbook*. ESDC

mission or operation also take into account the EU's security interests and are tailored to the local circumstances and to the tasks that need to be implemented.[253]


EUROPEAN UNION
CSDP OPERATIONS AND MISSIONS 2017
EUPOL COPPS Palestinian Territories Since 2006
EUFOR ALTHEA Bosnia Herzegovina Since 2004
EULEX Kosovo Since 2008
EU NAVFOR MED Since 2015
EUTM Mali Since 2013
EUCAP SAHEL Mali Since 2014
EUCAP SAHEL Niger Since 2012
EUTM RCA Central African Republic Since 2016
*EUBAM Moldova and Ukraine Since 2005
EUAM Ukraine Since 2014
EUMM Georgia Since 2008
EUBAM RAFAH Palestinian Territories Since 2005
EUBAM Libya Since 2013
EUAM Iraq Since 2017
EU NAVFOR Atalanta Since 2008
EUTM Somalia Since 2010
EUCAP SOMALIA Since 2012
Military Missions/Operations
Civilian Missions
6 on-going military Missions/Operations
10 on-going civilian Missions
More than 4,000 people currently deployed
Objectives:
keeping the peace, preventing conflicts strengthening international security, supporting the rule of law, prevention of human trafficking and piracy.
*This Mission is not managed within CSDP structures.

Picture 3. **CSDP Missions and Operations**[254]

There are currently 17 civilian and military CSDP Missions ongoing, and their tasks vary from capacity building and executive tasks to monitoring. There are more than 4000 people deployed and a remarkable portion of these are seconded by all EU Member States and from EU partnership countries. The mission or operation

[253] Common Security and Defence Policy Missions and Operations (2017). Annual Report. Retrieved from https://eeas.europa.eu/sites/eeas/files/csdp_annual_report_2017_web_en_2.pdf

[254] Ibid

mandate does not cover all aspects of the Integrated Approach and hence it is utmost important to work closely with other EU instruments, coordinated by EU delegation, in the field.

3. Successes of EU integrated approach

As earlier described, the Integrated Approach is a multi-disciplinary approach to influence the causes of crisis or conflict in the different phases. When the policies and strategies are developed in the Brussels, the implementation is largely depending on the work in the field. There are 139 Delegations representing the EU and its citizens around the globe, building networks and partnerships and promoting the values and interests of the EU. The delegations have a massive task to coordinate EU activities in the country. Furthermore, the CSDP missions and operations have their own reporting lines and chain of command, and delegations are not part of that. Despite of the wide variety of tools and activities of the EU response, there are multiple good experiences from the integrated approach in the field.

The cross-border security threats in the Sahel confirmed the relevance of an integrated approach to be taken in EU strategy. EUCAP Sahel Niger contributes through its mandate to the development of an integrated, coherent, sustainable, and human rights-based approach among the various Nigerien security agencies in the fight against terrorism and organised crime.

In the Horn of Africa three different CSDP missions and operations: EUCAP Somalia, EUTM Somalia and EUFOR Atalanta, are complementing each others' tasks and activities. But CSDP is not the only activity in the area, as there are numerous Commission funded financial and developmental programmes along with the political actions supporting the achievements of the EU strategic objective in the field. Furthermore, the EU is the biggest humanitarian donor to alleviate human suffering in the area. For financial actions, with the EU Trust Fund for Africa actions, worth of more than 800 000 million euros and more than 50 adopted actions, the EU is improving stability and addressing the root causes of irregular migration and forced displacement in the Horn of Africa region.

In Ukraine, the EU is unwavering in its support for the Ukraine's territorial integrity and sovereignty and sees the full implementation of the Minsk agreements as the basis for a sustainable political solution to the conflict in the east of the country. Since spring 2014, the EU has stepped up its support for economic and political reforms in Ukraine and is acting widely when supporting the peaceful settlement of Ukraine conflict. The EU is OSCE monitoring mission largest financial contributor and the European commission is managing tens of projects that are directly aimed to improve the infrastructure and administration of the Ukrainian authorities. All of these projects, as well as European Union Advisory Mission in Ukraine are part of EU Integrated Approach.[255]

[255] EU Ukraine factsheet. Accessed 15 March 2018. Retrieved from https://eeas.europa.eu/headquarters/headquarters-homepage_en/4081/%20EU-Ukraine%20relations,%20factsheet

Conclusions

1. The EU is a global actor in the field of security and it constitutes its actions to value based Integrated Approach to respond to conflicts and crisis. It is important to actively communicate on the policies and successes, as strategic communication is also an important part of the EU public diplomacy. As part of this, the EU is enhancing its strategic communications, which involves upgrading the consistency and speed of messaging on our values and actions. We offer rapid, factual rebuttals of disinformation, such as the EU Disinformation Digest analysis, as well as providing news on the European Union on daily basis.
2. The EU Common Security and Defence Policy (CSDP) allows the EU and its Member States to strengthen the civilian and military capabilities for conflict prevention and crisis management in a global level. The EU can and will act at all stages of the conflict cycle; on prevention, responding, investing in stabilisation and avoiding premature disengagement when new crisis erupts.[256]
3. Preparing personnel to the field missions that operate in the framework of the EU Integrated Approach, requires specific knowledge and multiple skills. Adapting these skills and knowledge, can lead to the expected outcome: adapting European security culture and European identity. The EU, as any organisation, is as strong and competent as its personnel is. Policies and strategies are implemented through people working in the missions, in the programmes and in the EU and Member States' structures. Multidiscipline international crisis management exercises, like the EU MultiLayer and VIKING, are excellent platforms to train personnel for the comprehensive approach. In

[256] Rehl J. (2017). *Handbook on CSDP – The Common Security and Defence Policy of The European Union*, 3rd Ed. Armed Forces Printing Centre, Vienna/Austria

exercises, different crisis management actors are solving problems, conduct joint analysis and planning, and learn how to interact in a safe learning environment. Exercises have been also identified as one of the areas of EU-NATO deeper cooperation.[257]

4. The EU has recently developed its rapid response mechanisms to respond to crisis and conflicts, such are the establishment of Crisis Platform and Immediate Action. Along the development of the responsiveness, the EU is constantly using the Integrated Approach to respond to the different phases of the conflict cycle. When using different instruments to achieve common goal, it is pivotal that the EU has a shared vision and that the EU instruments conduct a common analysis of the situation. Understanding of the EU instruments and functioning principles is important for all, not only for those who are working in the field of security in the EU missions, in the EU projects and in the EU structures – but also to all security stakeholders in the EU Member States.
5. EU has evolved over the decades to respond to the changing environment, and thus shown great adaptability and organisational learning. Recognising the threats that may challenge Europe and its citizens, is pivotal in this process. EU needs to constantly improve its performance in order to maintain competitiveness and commit, when necessary, to the new roles in this changing world. Other global actors, like USA, China and India will not necessarily share the views of the EU on how to best solve global security challenges. Therefore, as mentioned in the Global Strategy, it is necessary to bear in mind that United Nations is the sole global governing actor in the security.

[257] The Joint Declaration signed by Presidents of the European Council Donald Tusk, of the European Commission Jean-Claude Juncker and NATO Secretary General Jens Stoltenberg in Warsaw on 8 July 2016. Retrieved from http://www.consilium.europa.eu/media/24293/signed-copy-nato-eu-declaration-8-july-en.pdf

References

Boutillier C. (2017). The Security and Development Nexus. *CSDP Handbook*. ESDC

Buzan B. (1983). *People, States & Fear*. Routledge

Rehl J. (2017). *Handbook on CSDP – The Common Security and Defence Policy of The European Union*, 3rd ed. Armed Forces Printing Centre, Vienna/Austria

Serrano P. (2017). EEAS Crisis Response Mechanism. *CSDP Handbook*. ESDC

Tardy T. (2017). The EU: from comprehensive vision to integrated action. *EUISS Brief*, Issue 5

Council conclusions on Security and Defence in the context of the EU Global Strategy 9178/17 17 May 2017

Common Security and Defence Policy Missions and Operations (2017). Annual Report. Retrieved from https://eeas.europa.eu/sites/eeas/files/csdp_annual_report_2017_web_en_2.pdf

European External Action Service (2018). Factsheet. Retrieved from https://eeas.europa.eu

EU Comprehensive Approach to external conflict and crisis. *Joint Communication*, 11 December 2013

EU Ukraine factsheet. Accessed 15 March 2018. Retrieved from https://eeas.europa.eu/headquarters/headquarters-homepage_en/4081/%20EU-Ukraine%20relations,%20factsheet

A Global Strategy for the European Union (2016). Retrieved from https://europa.eu/globalstrategy/en

An Integrated Approach to external conflicts and crisis. 7 June 2017. European External Action Service 10054/2017

The Joint Declaration signed by Presidents of the European Council Donald Tusk, of the European Commission Jean-Claude Juncker and NATO Secretary General Jens Stoltenberg in Warsaw on 8 July 2016. Retrieved from http://www.consilium.europa.eu/media/24293/signed-copy-nato-eu-declaration-8-july-en.pdf

About the Authors

Kirsi Hyttinen, Master of Education, PhD cand
Kirsi Hyttinen is a Senior Manager for Research at the Research, Development and Innovation Unit at Laurea University of Applied Sciences located in Finland. Her work examines the EU's security environment, the effectiveness of EU's capabilities in conflict prevention, as well as expertise and professionalism of

peacebuilding and crisis management personnel. She has coordinated the Consortium of IECEU (Improving the Effectiveness of Capabilities in EU conflict prevention) –project and conducted the research in Gaming for Peace –project. Both of these projects are funded by the European Commission H2020 programme. She has also worked five years for national training provider for civilian crisis management personnel. Beyond these, her research interests focus on learning, adult education and information technology from cognitive point of view.

Petteri Taitto, Master of Education, General Staff Officer
Petteri Taitto is currently holding a position as Principal Scientist at the Laurea University of Applied Sciences, Finland. His job includes peacekeeping, peacebuilding and humanitarian response project development and coordination.
Taitto has earlier coordinated EU CSDP Mission related training programmes at the European Security and Defence College (EU Brussels), tailored and implemented various training programmes as CMCFinland Head of Training and been teacher at the Emergency Services College and at the National Defence University.

WHISTLEBLOWING – GROWTH OF SOCIETY

Jānis Veinbergs
Vilnis Veinbergs

Introduction

We must be aware that each unique social individual, only ourselves and each and every one of us is responsible for himself/ herself, for our own children, for the environment we live in and for the heritage we leave to the next generations, which will inevitably reveal the beliefs, opinions and values of the previous generations.

The general indifference dominating the society, its reluctance, fear or lack of courage to interfere immediately with illegal actions and to stop them and, quite often, also the lack of understanding of the issue, precludes it from taking action against dishonest or illegal activities. This reality allows and quite often encourages action or inaction of individuals or groups, which manifest themselves as a threat against us or evil.

For the purpose of initiating reflection: what are the most frequent actions people take when sensing a threat? What are the motives, which make the public unprepared for engagement and taking action against dishonest activities that threaten it? What methods does a democratic country possess in order to fight against fraud? What needs to change for each of us that would make the public say that “one must not cheat”?

These are just some of the questions which should be contemplated by everyone and we should assess our own future attitude and actions in order to be capable of living in a self-sufficient, honest, responsible and growth-oriented society.

A state is a system, which has been created by the society for the purpose of honest public governance. The first state structures that we are aware of date back to the Ancient Greece. “The early Greek society was quite simple – the community was initially formed by a few hundreds or thousands of people, who had joined together on the basis of their overall coherence and fixed collective laws”.[258] Already in the Ancient Greece, a lawful and fair cohabitation of people for a just running of their collective property was the cornerstone of their Poleis’ formation. One should also take into account the fact that the society of the Ancient Greece was not divided on the basis of material or financial values. During that period there was no explicit distinction between richer and poorer members of its society. At that time people were living “hand to mouth”. Money, which was first introduced in late 7th century BC and which replaced cattle as the means of payment, became the main payment instrument, which determined the social status of a person. “Money makes a man”.[259] This saying became a motto of the time. Today, we can define the core values of capitalism in similar terms, which substantially affect human thinking and the goal of becoming a “successful” person. The introduction of money as the means of payment slowly shifted the existing pillars of the early Ancient Greece: family nobility, warrior courage, individual intellectual ability and character traits.[260]

The three virtues of excellence proposed by a contemporary thinker Otfried Höffe, which are based on Ancient Greek philosopher

[258] Rubenis A. (1998). *Senās Grieķijas kultūra*. Rīga: Zvaigzne ABC, p. 27

[259] Ibid

[260] Ibid;

Klišāne J. (1998). *Senā Grieķija*. Rīga: Zvaigzne ABC, p. 12

Plato's (428.–348 BC)[261] three main forces of the soul: the appetitive, spirited and rational. For appetitive Höffe proposes composure, for spirited – courage, for rational – comprehension or wisdom, which according to the author successfully characterise an honest member of a society and these should be the qualities of a whistleblower or a fighter against crime.

Along with the rise of the first state (Polis), there was a necessity for the formation of laws and regulations, which were written down on the basis of verbal dictation. "Along with written publication of laws and books they became a property of the society as a whole. For general knowledge, laws were carved in stone, claiming their role as a higher level of truth belonging to everyone".[262]

It should be taken into account that the system itself and the aggregate of people, who have been entrusted with the rights of organising life of a society, do not earn money themselves. Money, which flows into the system is taxpayer money, it is administered within the state system by individuals appointed by the public.

At the 1983 Conservative Party conference the former British prime minister Margaret Hilda Thatcher, who undoubtedly is one of the most important personalities of the 20th century, said the following words: "Let us never forget this fundamental truth: the State has no source of money other than money which people earn themselves. If the State wishes to spend more it can do so only by borrowing your savings or by taxing you more. It is no good thinking that someone else will pay – that "someone else" is you. There is no such thing as public money; there is only taxpayers' money."[263]

[261] Kūle M, Kūlis. R. (1996). *Filosofija*. Rīga: Burtnieks, p. 163

[262] Bojārs J. (2002). *Politiskās stratēģijas māksla un demokrātija*. Rīga: Zvaigzne ABC, p. 115

[263] Thatcher M. H. (1983). Conservative Party conference. Acquired from https://www.margaretthatcher.org/document/105454

There are numerous known cases when public funds are not managed in accordance with public demands when they are purposefully mismanaged or simply stolen.

In situations like these they get into the hands of dishonest people and instead of serving the development of society and its future stability, they serve the selfish materialistic interests of such people.

What should be done for the purpose of achieving a society dominated by honesty, justice and responsibility? It is necessary to be aware that we have to take care of it only by ourselves. Actions like "standing by" or not interfering in actions targeted against public interests do not constitute the mentality of a responsible society.

Unfortunately, history holds many examples when people have tried to reach their personal materialistic goals in the name of openness and promotion of responsibility and it is exactly those negative whistleblowing examples that are often put to the forefront. Is the use of such examples and thus promoting a view in the public that whistleblowing is a shameful activity and that one has to keep silent an honest approach? What is our own responsibility for ourselves and our future?!

For the purpose of raising the activity of whistleblowers, it is necessary to understand those motives, which impede it, the motives which make the society unprepared for engaging in the promotion of openness as well as to emphasize the motives, which promote the activity of whistleblowers.

Along with the task of developing the systems of security and internal control of organisations, it is fundamentally important to promote the prevention of economic infringements and their eradication by preventing money laundering as well as to facilitate countermeasures against the shadow economy. All of this can be called a precondition for the existence and development of a democratic society.

The authors ask the readers to learn those motives, which determine the readiness or unwillingness of the public to engage in the promotion of openness and responsibility as well as to learn the historical experience in the fight against "evil" and the development of the whistleblower movement in Latvia and other countries of the European Union.

1. On whistleblowing

The assessment of the compliance of Latvia with the requirements of the United Nations Organisation (hereinafter – UN) Convention Against Corruption by the Conference of the States Parties to the UN Convention Against Corruption, which took place on June 2–6, 2014, resulted in a recommendation to develop a comprehensive and specialised legal regulation for the legal protection of whistleblowers.[264] Based on this recommendation, the Republic of Latvia (hereinafter – LR) has worked out a draft law "On the Protection of Whistleblowers". The draft law was presented and discussed at the international conference "Towards openness, responsibility and better governance: the promotion of whistleblowing, the fight against corruption, future prospects" on 8–11 October 2017.[265]

[264] Conference of the States Parties to the United Nations Convention against Corruption. Acquired from http://www.unodc.org/documents/treaties/UNCAC/WorkingGroups/ImplementationReviewGroup/ExecutiveSummaries/V1401272e.pdf

[265] Towards openness, responsibility and better governance: the promotion of whistleblowing, the fight against corruption, future prospects. International conference. Acquired from https://www.mk.gov.lv/sites/default/files/editor/trauksmes_celeju_konferences_programma_v1.12.pdf

Draft law "Law on the Protection of Whistleblowers" approved by the Cabinet of Ministers on 7 March 2017. [266] The objective of the draft law is to develop, support and promote whistleblowing in the public interests. The draft law defines the notion of a whistleblower and the meaning of a whistleblower by establishing the requirements for developing internal mechanisms of whistleblowing in a systematic manner. It outlines the measures for whistleblower protection by guaranteeing anonymity and ensuring that creation of any unfavourable consequences for whistleblowers are prohibited.[267]

1.1. Who is a whistleblower and what conditions requires whistleblower activities under the law

Under the draft law, a whistleblower is a person who raises public alarm regarding violations at his/her workplace. Raising of alarm, for instance, regarding embezzlement of financial or materials funds, tax evasion, risks to public health and threats to environment safety or construction constitutes legitimate public interest.[268]

This leads to a conclusion that a whistleblower is a person acting in good faith, who discloses information on a violation, which can be harmful to public interests or the interests of part of the public. It is a person who, by defending his/her interests, the interests of the general public and the interests of the next generations, does

[266] Law on the Protection of Whistleblowers Draft law, reviewed and promulgated on 17.12.2015, MK 07.03.2017, acquired from http://tap.mk.gov.lv/lv/mk/tap/?pid=40377799&mode=mkk&date=2017-02-06

[267] Explanatory memorandum of the cabinet of Ministers, Law on the Protection of Whistleblowers. Draft law. Acquired from https://webcache.googleusercontent.com/search?q=cache:PBo7yM_PDeIJ:https://www.mk.gov.lv/lv/content/trauksmes-celeji+&cd=1&hl=lv&ct=clnk&gl=lv

[268] The course of development the specialised legal regulation on whistleblowing. Acquired from https://www.mk.gov.lv/lv/content/trauksmes-celeji

not remain indifferent and engages in the protection of the society and fights against violations as an evil by legally available means.

The draft law points out the types of violations, which are in breach of public interest:

1) embezzlement of financial or material funds by a public official;
2) fraud;
3) inaction, negligence or abuse of power by the responsible officials;
4) corruption, including bribery of foreign public officials;
5) threats to public health;
6) threat against food safety;
7) risks to construction safety;
8) threat to the environmental safety;
9) public procurement violations;
10) breaches of labour safety;
11) tax evasion;
12) violations in the area of finance and capital market;
13) other violations.[269]

If we wish to redefine this list in just a few words, they would consist of three characteristics:

1) dishonest/improper use of the entrusted legitimate power or rights;
2) bribery as a method for achieving greater advantage in respect to other members of society;

[269] Law on the Protection of Whistleblowers Draft law. Reviewed and promulgated on 17.12.2015, MK 07.03.2017, acquired from http://tap.mk.gov.lv/lv/mk/tap/?pid=40377799&mode=mkk&date=2017-02-06

3) fraudulent action by using inadequate information or non-disclosure of information for the purpose of reaching personal materialistic gains.

There are always definite people behind the indicated manifestations or actions who can be divided according to their roles and consequences of action. These roles are:

1) interested parties and employees;
2) aggrieved parties and parties who have suffered losses;
3) observers or witnesses.

In any situation, each of us, willingly or unwillingly, falls into one of the aforementioned roles.

1.2. Obligations, rights, responsibility and protection of a whistleblower

Our rights, obligations, responsibility and even the course of action are included in the respective laws. There are many laws – almost 15,000 of them, and only professionals are capable of knowing them well. Nevertheless, it is not that difficult for any individual to find and clarify the needed norm, which is often the one that can turn out to be crucial. It is well known that ignorance of laws or Cabinet of Ministers regulations does not exempt anyone from liability.[270] At this moment there are already norms of several laws, which in certain cases envisage liability for the failure to report on violations. Any individual can be administratively or criminally

[270] The Law on Official Publications and Legal Information. Adopted on 31.05.2012, *Latvijas Vēstnesis*, No. 96 (4699), 20.06.2012, Latest amendments 10.12.2016

liable for non-reporting.[271] For instance, Article 46.3 of the Administrative Violations Code of Latvia defines liability for a failure to report on the medical product advertising activities, while Article 88.8 establishes liability for a failure to provide information up or down the supply chain on chemical substances or chemical substances in mixtures as well as for a failure to report on substances in products not requiring a safety data sheet. Article 165.10 establishes liability on failure to inform the respective institution defined by law on suspicious deals involving such substances, on their theft or loss which is required under normative acts regulating sale and use of explosives precursors, etc. Responsible employees must also report on suspicious financial transactions. A civil servant must inform in case of doubt about the legality of his/her duty assignment. In a similar way, laws also stipulate the requirement to report on an existence of a conflict of interest. One must always take into account that our rights and responsibilities exist in parallel with the legal norms establishing our obligations.

To paraphrase the recognised Latvian poet and playwright Jānis Pliekšāns (Rainis, 1865–1929). "Each of us must lend a hand to see a greater good succeed!"[272]

The main objective of the legal framework stipulated by the draft law "On the Protection of Whistleblowers" is to ensure whistleblower protection and to promote whistleblowing on violations in state institutions and legal employment relationships by forming a unified and comprehensive legal regulation for whistleblowing and whistleblower protection, which contains:

[271] Administrative Violations Code of Latvia. Adopted on: 07.12.1984, *Ziņotājs*, No. 51, 20.12.1984, Latest amendments 04.07.2018

[272] Rainis – poet, playwright. Acquired from http://www.aspazijarainis.lv/par/rainis/

1) a clear definition of who is a whistleblower and what constitutes whistleblowing;
2) a requirement to form the internal mechanisms for whistleblowing in a systematic manner;
3) common basic requirements for competent public authorities for processing whistleblower submissions;
4) duties related to the protection of whistleblowers:
   - anonymity;
   - prohibition to cause negative consequences;
   - elimination of negative consequences, including court procedures;
   - liability for causing negative consequences for a whistleblower.[273]

There is no secret that quite often upon learning about their liability persons engaged in an incident are interested to discover the name of the whistleblower. And also to get to know how has the whistleblower learned about the violation?

Thus, they want to know who that person is and not because they want to say thank you.

Corruption as an initiator, a constituent part of the process and its consequence is dominating among the types of violations listed in the draft law, which are in breach of public interest.

Corruption (Latin *corruptio* damage; bribery) – use of an official position for selfish goals; corruptibility of public officials.[274] In the law on the Corruption Prevention and Combating Bureau

[273] Law on the Protection of Whistleblowers Draft law. Reviewed and promulgated on 17.12.2015, MK 07.03.2017, acquired from http://tap.mk.gov.lv/lv/mk/tap/?pid=40377799&mode=mkk&date=2017-02-06

[274] Autoru kolektīvs. (2005). *Ilustrētā svešvārdu vārdnīca*. Rīga: Avots, p. 397

(KNAB), corruption is defined as “bribery or any other action by a public official targeted at gaining undeserved privilege for himself/ herself or other persons by means of using one’s official status and authority or by abusing those powers".[275]

Corruptive activities or relations are possible in several forms, for instance, as administrative corruption, political corruption, et al. Destructive attitude of the executive power or decision-making power towards the general public. Corruption leads to the expansion of shadow economy, increase of social inequality and slowing down of the democratic development of a society. All law enforcement institutions of Latvia are engaged in fighting corruption, including the Corruption Prevention and Combating Bureau.[276]

Creation of any goods or values requires resources, which are compensated by the consumer of those goods and values. It also includes salary paid for the creation, accounting, storage and consumer distribution of the goods and values. Tax based public value as a property of all the society is one of such values or goods. In order to administer these values, the public authorises its representatives to act as administrators/civil servants entitled with the rights and obligations as a totality of actions based on law.

In this situation one must be aware of two substantial issues:

1) The conservative nature of law. Legislation represents the use of a real negative case in order to establish the necessary measures as a responsibility targeted at reducing the growth of violations. At the same time, the law cannot predict all possible variations for evading the law. For good reason: there is a saying that “law is like a

[275] Korupcijas novēršanas un apkarošanas birojs (2018). Korupcija. Acquired from https://www.knab.gov.lv/lv/education/forschools/

[276] Ibid

telephone post, which cannot be stepped over, but which can be bypassed";

2) Possibilities of control. It is not possible to establish a comprehensive control over civil servants as authorised supervisors of public goods. It would require a disproportionate amount of administrative resources, it would affect the quality of work of authorised supervisors of public goods/civil servants or would preclude creative personalities from working in the area of management public goods. Therefore, administration or management of public goods retains in itself a potential for corruptive actions.

The primary causes of corruption as an evil:

1) the possibilities for interpretation of laws due to their ambiguous nature;
2) the lack of understanding by the public, e.g. lack of knowledge on the obligations and rights of civil servants;
3) unstable economic or political situation;
4) different operation of state institutions in defining in and reaching public goals;
5) changes in the standards of operation and those principles, which are formed by political elites for their own necessities;
6) incompetence of civil servants;
7) the existence of aligned goals within various political groupings and executive circles, causing various mutual agreements on convenient variations of control and cooperation;
8) disengagement of the public from the anti-corruption policies.

There are also other, so-called, hypothetical reasons for the existence of corruption:

1) low wages in the public sector compared to the private;
2) alienation of the bureaucratic elite from the general public (the well-fed does not understand the lean);
3) ethical stratification of the society;
4) stagnation and slow economic growth;
5) traditions.

Corruption as an evil can manifest itself in various fields, for instance, in the form of threats to public health, food safety, services offered by the construction industry, environmental safety, et al.

It manifests itself as threats to public health in cases when those people requiring emergency or long-term medical treatment fail to receive it or do not receive it on time due to the fact that it is, first of all, offered to those who have paid with full envelopes and by other "means of gratitude", thus gaining privileges. It is also the issue of medical drugs, which, despite their task of maintaining and improving our health, can be not only improper but also harmful or fake.

Food security is related to all of its producers and suppliers, as well as retailers, wholesalers and consumers. The producer wishes to produce more and at a lower cost, while retailers wish to sell to gain profit. This may lead to the production of poor quality and even harmful items, which nevertheless hold all the required quality certificates and trade permits. A consumer unknowingly buys something obscure, unknown, which can be harmful to health or even life-threatening.

Construction safety risks are related to the desire to build faster and cheaper.

The vigilance and engagement of people has triggered processes which have led to constant elimination of violations in the field of construction. However, this vigilance, unfortunately, started only after the tragedy at Zolitūde (collapse of "Maxima" supermarket in Riga, referred to by the media as Zolitūde tragedy, occurred on 21 November 2013). Public participation is one of the key preconditions for state development. Successful cooperation between public administration institutions and general public serves as an important example of identification of problems and finding their solutions and for the overall development of the construction industry. The public initiative on construction proposal review proves that paying attention to the issue and promoting discussion on construction related issues provides an opportunity to eliminate violations in a timely manner and correct systemic mistakes without waiting for a negative end result as it had happened up to now. Whistleblowers report on possible violations at construction sites by asking to clarify if a particular construction process has been agreed upon in accordance with the law. People also report on building deformities they have noticed or signs which can indicate that the building can possibly cause harm to people's health and lives. Reports are also filed on illegal employment and tax evasion in this regard.

Possible threats to environmental safety represent a direct threat to our livelihood. It is the air that we breathe, the ground that we walk on and the water that we drink. There is no alternative. It simultaneously represents our health and vitality.

Violations can also manifest themselves in the areas of public procurement, disregard for labour safety, tax evasion as well as violations in the financial and capital market sector.

2. The image of a whistleblower in the cultural and historical heritage

What is a whistleblower, what is a whistleblower's mission and calling? How were whistleblowers viewed by previous generations? How did they call whistleblowers?

"Whistleblower" is a new term in the historical context. It is essentially an individual, who raises alarm and is a fighter against evil. A whistleblower fights for justice by means and methods available to him/her. Courageous people are not always completely understood, but they are exactly those, who have sacrificed themselves in the name of noble goals important to all humanity.

Today's situation proves that there is a lack of courageous people. It is particularly true regarding the current moment when the society is saturated with information on entertainment and unrealistic opinions. Courage is also a manifestation of one's personality, required by everyone in order to understand one's place in the society and to be capable of seeing the individual responsibility expected from an individual by the society as a whole.

The development of humanity is based on heroes and characters, which have advanced the development process through the centuries. At least once in a lifetime, every person has contemplated the importance of religion, its power and values, which various religions promote as important. Analysing poetry, folk-tales and other written works one has to conclude that those easily comprehensible yet at the same time complicated works have hidden the code of human action and success, which needs to be understood and put into use.

2.1. Religion as a teaching on morals and ethics

Religion is a totality of views and beliefs related to something supernatural, sacred or divine. It also represents morals, customs, rituals and organisations connected to it. In religion violations have only one characterisation: sin.

In Christianity the Roman Catholic Church teaches that the seven deadly sins are:

1) pride [superbia];
2) envy [invidia];
3) wrath [ira];
4) sloth [acedia];
5) gluttony [gula];
6) lust [luxuria];
7) greed [avaritia].[277]

Saint Gregory the Great (Bishop of Rome from 590 to 604 AD) called these seven sins as cardinal or deadly sins. Many years later Tomas Aquinas (1225–1274) in his work "Summa Theologiae" explicitly singled out two sins: greed or stinginess and pride or ambition.[278]

The beginnings of fraud and corruption are directly linked with a desire to obtain something that a person does not have a right to hold and the desire to obtain it as much as possible. Without creating the respective material values themselves, by being lazy and becoming envious and even malevolent and angry they start to

[277] Pāvesta kārtējie septiņi nāves grēki. Acquired from http://www.ebaznica.lv/pavesta-kartejie-septini-naves-greki-3695/

[278] Riekstiņš. K. (2004). *Kas ir septiņi nāves grēki un atbildes uz vēl 53 erudīcijas jautājumiem*. Rīga: Avots, p. 52

ignore the principles of equal distribution of public goods. This results in pride in one's capabilities to be superior to others.

The Ten Commandments or, as they are called, Decalogue – the ten notions have been used in the Old Testament almost without changes in the Book of Moses and they stand as a synopsis of the divine teachings on what we have to do in order to make our lives liked by the God. It is believed that this is the true source and the beginning of all good deeds. No work or action can be good and liked by the God if they are not based on the compliance with the Ten Commandments.

"Let us see now what our great saints can boast of their spiritual orders and their great and grievous works which they have invented and set up, while they let these pass, as though they were far too insignificant, or had long ago been perfectly fulfilled".[279]

At this time when the contemporary man lives under the pressures of creative hurry and various drives and inclinations, the historically traditional attitude and scale of values towards religion as a moral and ethical teaching has been changing. Nevertheless, it has not disappeared.

Vatican has acknowledged that the contemporary trends of the commercial world cannot be ignored since the development of economy brings along the development of sinners who have to repent:

1) genetic modification;
2) experimentation on humans;
3) creation of social injustice;
4) causing of poverty;
5) excessive wealth;

[279] Desmit Dieva baušļi. Acquired from http://www.janabaznica.lv/luters/martina-lutera-lielais-katehisms/desmit-dieva-bausli/

6) drug abuse;
7) pollution of the environment.[280]

Studies on the views and positions of young people were conducted in seven European countries. Their results were published in a Swedish Christian paper "Dagne". The age of respondents ranged from 16 to 34. In the course of five months 7,000 young people from the UK, Germany, Italy, the Netherlands, Poland, Greece and Sweden shared their views about themselves. These studies reveal that the contemporary youth is highly individualistic compared to the previous generation. This does not mean that they do not value the importance of tolerance and compassion in life. According to the young people surveyed, alcohol and drugs are an inalienable part of their lives. However, it is obvious, that many young people do not like drugs and everything related to them. The young people stress that there is a big difference between their own attitudes towards themselves and the way and perspective they are depicted by the international media. They reject the "old" perceptions that they are lazy, rebellious and obsessed with celebrity worship. Many of them rather view themselves as hard-working, optimistic individuals who are friendly towards their peers. Influence of parents on the formation of attitudes and assessments is also viewed positively. Family life is a value one can strive for.[281]

Weighing all the pros and cons, the results have been summarised as ten new "commandments" and seven "deadly sins".

[280] Desmit Dieva baušļi. Acquired from http://www.janabaznica.lv/luters/martina-lutera-lielais-katehisms/desmit-dieva-bausli/

[281] Mūsdienu jauniešu jaunie 10 baušļi un 7 nāves grēki. Acquired from http://www.lkr.lv/lat/kristigas_zinas/pasaules_zinas/?doc=61

1. The ten commandments are:
    1) trust yourself;
    2) respect your parents;
    3) be honest;
    4) take charge of your own life;
    5) live your life to the full and feel it;
    6) keep your promises;
    7) work hard yourself to succeed but don't do it at the expense of others;
    8) be tolerant towards the differences in other people;
    9) be happy and optimistic, even when facing failures;
    10) be a creator, not a destroyer.
2. According to the contemporary youth, the seven new "deadly" sins are:
    1) racism;
    2) dishonesty;
    3) mobbing (doing harm to others by various means – physical and psychological);
    4) avarice, gluttony, greed;
    5) cheating, adultery;
    6) anger;
    7) envy.[282]

Therefore, one can conclude that the understanding of the Sin as an evil has been preserved. It clearly changes, because the conditions of human life are changing as well. Our relations with religion are seemingly smarter. However, deep in our hearts, are we

[282] Mūsdienu jauniešu jaunie 10 baušļi un 7 nāves grēki. Acquired from http://www.lkr.lv/lat/kristigas_zinas/pasaules_zinas/?doc=61

ready to stand against the Almighty and choose to defend the evil? A whistleblower in his/her very nature is a fighter against evil.

2.2. Folk-tales as a depiction of past experiences

Folk-tales are a retrospect into the well-wishes of the past, which are directed at us as the upcoming generations. Folk-tales are small works of prose, which are mostly written for children. The role of characters in folk-tales is usually set in wonder worlds, seemingly unreal environments, which have been purposefully constructed different from the life that we know, with unknown laws of physics, impossible things and places as well as supernatural beings and abilities.

Folk-tales and legends have come to us, yet we do not know from which immemorial times they have arrived. We cannot establish their geographical birthplace either. They can be compared to the, so-called, ethnographic signs. Those ethnographic signs, which we refer to as Latvian or more broadly – Baltic, can be found in the ethnography of all Northern nationalities. These ethnographic signs represent an ethnographic testimony of national identity of Scandinavians, the peoples of Russian north as well as the indigenous people of North America. The same applies to folk-tales and legends. The meaning of Latvian names like "pasaka" (a folk-tale), "teika" (a legend), and "teikt" (to say), "pateikt" (to tell) are semantically identical.

In Russia, they say "сказка", which stems from words "каза́ть" or "казка". In translation, it means "to say" or "to point out".

Folk-tales represent spoken messages from an unknown past, which appeared in writing only in the 18th century. At that time these messages were already nationalised by including place-names of specific regions: toponyms, hydronyms and oronyms.

Similarly to pearls, which in the beginning are just a grain of sand, a folk-tale in its essence is possibly a depiction of actual events with supporting realisations, which has been brought to us from the past. By deciphering ancient folk-tales, we can recognise all the traits of modern technology, equipment and problem situations.

Maybe everything that folk-tales tell us has already happened before?

The creativity of people and their capacity to fantasise are limited. Fantasies are a result of the process of imagination based on symbiosis of various types of information. Prof. P. Šmits writes the following: "The explanation presented to us by folk-tale researchers that many wonderful motives of legends are derived from real-life events does sound strange to us, but we are in doubt only because we do not understand the superstitions of ancient people and their fear of various ghosts and weird creatures".[283]

There are various types of folk-tales of Antti Aarne. Their main heroes can be animals, people or supernatural creatures alien to us, movable and verbalising items, etc. Assessing folk-tales and doing so even superficially, without dwelling into their psychological and philosophical analysis, one must conclude that all of the tales provide a single conclusion, i.e. that the history of a hero against evil implies courageous and selfless action, sometimes by sacrificing one's own life.

This leads to a conclusion that the fight against threats has existed during all times and that victory is ensured by courage to start a battle and fight with a clear realisation of the goal as a precondition for the existence of society and future generations.

[283] Pasaku un teiku pamati. Acquired from http://valoda.ailab.lv/folklora/pasakas/ievads04.htm

2.3. Fiction as an element of self-education of society

"The Divine Comedy" (Italian: La Divina Comedia) written by Italian poet and philosopher and one of the founders of the Italian language Dante Alighieri or Dante (May 1265-13/14 September 1321) should be noted as a vivid example in this context.

The paradigm of "The Divine Comedy"[284] embodies a definite model of perception and thinking, a view of the world and a theoretical assumption of responsibility. Although the imagery and the allegoric view of the afterlife is a culmination point of the developed medieval philosophy of the Roman Catholic Church, "The Divine Comedy" directly and unmistakably points to those manifestations of human actions, which must be viewed as conscious evil with an allegorical culmination of responsibility for it. In "The Divine Comedy", which has become part of the most prominent cultural canons of humanity, Dante imaginatively describes a middle-aged person who has entered a situation of deep contemplation and uncertainty. In a dream, he has been given an opportunity to see the consequences of sins/violations. His companion leads him to a large conical – shaped ravine referred to as "hell". The hell has nine circles.

The circles up to the fifth circle contain the passive sins (denoting indifference and the lack of willpower). There is Limbo – a waiting room occupied by pagans and non-Christians, Islamic philosophers and the Antique classics. It is a location of green meadows and castles.

Beyond the first circle resides Minos, the Infernal judge (a legendary King), who judges souls.

The second circle is Lust – a place for those who succumb to lust. This circle is dominated by eternal winds and storms.

[284] Autoru kolektīvs (2005). *Ilustrētā svešvārdu vārdnīca*. Rīga: Avots, p. 542

The next circle is Gluttony, both: as excessive eating or any other excessive form of dependence. The circle is dominated by an eternal rain and hail – sleet. This circle is guarded by the worm-monster Cerberus (in Greek and Roman mythology it represents a dog with several, usually three, heads).

The third circle is followed by Greed and Profligacy, where the greedy and the wasteful push heavy stones as weapons against each other.

The fifth circle is occupied by the angry and the sullen on the waters of Styx, which encircles the Underworld nine times separating it from the world of the living, as well as on marshes. The sullen sleep there, while the wrathful fight one another.

Active sinners occupy the circle from the 6th to the 9th.

The sixth circle is the circle of Heresy and is depicted as burning tombs, where the heretics (promoters of various false teachings) and Epicureans (who believed that life was formed by accident) burn in eternal flames. It is the place for all those who believed that soul dies along with a physical body and that there was no afterlife.

The seventh circle is resided by those who have performed violent deeds. It houses a river of boiling blood soaking tyrants and murderers. These “people” are chased by dogs. Those who have committed suicide have been turned into thorny bushes and trees. And this is also the place for those who have committed blasphemy. Those who have slandered and ridiculed others, their feelings or convictions. The circle is also resided by sodomites who walk the desert of burning sand and flaming flakes, which fall from the sky. The blasphemers are lying on the ground, while the sodomites must walk around in groups. This circle is guarded by Minotaur (a creature in the Ancient Greek mythology with the head of a bull and the body of a man).

The eighth circle contains ten stone ditches or “bolgias” (Italian for pouch or ditch). The first bolgia contains seducers guarded by demons (supernatural evil creatures). The second bolgia is the place for flatterers and toadies who are immersed in excrement. The third is the residence of high ranking priests who have traded church offices and positions. Their feet are set ablaze by fire. Today those people would be political ideologists and government officials. The fourth bolgia consists of astrologists, false prophets and magicians, whose heads are turned around, thus making them walk in the opposite direction. The fifth bolgia is the residence of grafters who are thrown into a river of boiling pitch. The sixth bolgia deals with the punishment of hypocrites who are forced to wear heavy led hats, which crush their minds.

Thieves are located in the seventh bolgia and they must suffer the bites of serpents.

People who have given corrupted advice and used their position to make people believe in lies must eternally burn in the eighth bolgia.

The ninth bolgia is the residence of instigators – those people who promoted scandals (nowadays those would include revolutionaries).

And the last one is called betrayal – the most evil of all bolgias.

Here the sinners face an eternal cold and ice.

The bolgia itself has four subdivisions or circles for those:

1) who betrayed their families;
2) who betrayed their cities and states;
3) who invited guests and killed them;
4) who betrayed their superiors.

They all are completely frozen in ice.

The bolgias are followed by Purgatory for those who have committed any of the seven deadly sins.

The sins are pride, envy, sloth, avarice, gluttony, lust and wrath.

In "The Divine Comedy" Dante Alighieri points to the four cardinal virtues:

1) prudence;
2) justice;
3) temperance;
4) fortitude.

Although Dante created "The Divine Comedy" 700 years ago, the list of human sins or moral and ethical drawbacks has not changed. But how about responsibility? The manifestations required to a whistleblower have not disappeared either. Prudence when assessing a situation, a sense of justice as a constant value, moderation at decision-making and courage in action.

The Latvian literary heritage also contains enlightening and interesting masterpieces. For instance, the 1879 novel "Mērnieku laiki" ("The Days of land Surveyors") by brothers Reinis Kaudzīte (1839–1920) and Matīss Kaudzīte (1848–1926).

It was the first realistic novel published in the Latvian language. In this novel, we can recognise fraud, inaction by responsible officials, negligence and abuse of power with corruption and bribery. The novel depicts events in two fictional parishes of Vidzeme region of Latvia at the time of arrival of land surveyors who are tasked with re-measuring and dividing plots of land belonging to the local manor. The prototypes of the places and heroes of the novel are from Piebalga region where both authors resided at the time.[285]

[285] Par brāļu Kaudzīšu romānu Mērnieku laiki. Acquired from https://letonika.lv/literatura/Section.aspx?f=1&id=2191065&r=160

One of the authors Reinis Kaudzīte gladly visited a local pub, sat in some darker corner and observed the locals argue, make friends and share drinks. After returning home he told his observations to his brother Matīss, who was more gifted at eloquently putting it in writing. They often re-read their texts and discussed them, deciding on what to keep and what to omit. The novel or, as the brothers themselves called it – living pictures, was written by both of them and they equally shared both – praise and criticism. The idea that the character prototypes were chosen locally in Piebalga has been proven by the fact that there were many prototypes of the main characters in Piebalga: there were nine offended and morally bruised Ķencis, three prototypes of Pietuka Krustiņš and also one of Švauksts. But how many naive Ķencis are there today?

A Latvian writer, journalist and translator Pāvils Rozītis (1889–1937) has also given his readers similar realistic novels: "Ceplis" and "Valmieras puikas" ("The Boys of Valmiera").

In the novel "Ceplis", one can recognise some of the contemporary business methods. The action of the novel takes place in Riga in the 1920-ies. An enterprising man establishes a joint stock company for exporting bricks made of Latvian clay. Many people join his project, hoping to make profit. Soon it becomes clear that the clay is not usable in brick building due to its inferior qualities. Before anyone learns it, schemes were made to make sure that the unprofitable stocks were sold and those who believed that they had become co-owners of a promising and profitable company lose out. These kind of deals are quite widespread also today. The saying "nothing personal, just business" is used for a good reason.

Another novel written by Pāvils Rozītis called "Valmieras puikas" is an autobiographical work related to the events in

Valmiera at the time of 1905 revolution. It is a story of how false advisers and instigators of rift (in modern days – revolutionaries) abuse the trust of teenagers for the sake of their own political and materialistic goals. It is not a secret that those revolutionaries had acquired the knowledge of instigation in order to use them for igniting the fire of global revolution. The monument erected at the banks of River Daugava and devoted to the victims of 1905 revolution stands as a symbol of shame and warning.

3. Whistleblowers and their motivation to report or not to report

Working at a state institution and receiving information on various violations as well as cooperating with those who provide such information, one comes to certain conclusions on the issue of whistleblowing and whistleblowers.

They are our compatriots who, by providing information, truly wish to assist the authorities in addressing the violations defined in the draft law. They do not view themselves as informants or whistleblowers. The motivation to provide information is based on their desire to fight violations as evil.

It is demeaning and sordid to refer to them as “snitches”. Usually, this choice of words comes from people who do not understand the notion of shared responsibility about the current and future threats and signals about their indifference about future. Or they are those persons who are afraid that their negative actions, support of such actions or inaction could be made known to others and they would have to face the consequences.

Quite often the demeaning slang word used in Latvian for a whistleblower is a Russian word “stukač”. It is a relatively new name. In translation, it means “a knocker”. It appeared at the end of

19th century in Russia together with “народовольцы – Народная воля – революционная народническая организация” (Russian) (“representatives of people’s will” – “Will of the People – a revolutionary popular organisation), which actively used terror as a method.

The goal of these active users of terrorist methods was to instigate terror in the country by murdering civil servants of the Russian Empire and to initiate panic. They successfully assassinated Tsar Alexander II as well as many civil servants of the Russian Empire. They were supported by Polish and other Western reactionary circles and a segment of Russian intellectuals of that period. Taking into account that they posed a threat to the Empire, active counter-measures against them were implemented. When imprisoned, these “народовольцы” (representatives of people’s will) quickly agreed to cooperate with the security structures of the Russian Empire. In order to avoid captivity, they were ready to tell everything about everyone. At that point, the derogatory term “stukač” came into existence, since the intellectuals – representatives of people’s will said: “it is better to knock about our own people than to knock on the wall of the neighbouring cell”.

Today, the contemporary society are not just informants on illegal activities of other people for the purpose of avoiding prison due to their failure to provide a timely report on crimes to the law enforcement authorities. The contemporary society demands tangible, real and regular action from the government in order to contain and eradicate criminality, embezzlement of public property and eradicate obstacles to the state development.

3.1. Five reasons why members of general public do not wish to report on evil

1. Fear, because people are not sure about the preservation of their anonymity.

One must really think before providing information to somebody else. It is probably better to report to an official person, authorised to handle such information as opposed to pouring out one's heart to a "good" acquaintance.

Information leakage usually takes place due to three factors:

- a tendency to chit-chat since many of us wish to attract attention and pretend to be smarter than we really are. In these manifestations, we replace our lack of real knowledge with something "extra" that we think that other people do not know. This "extra" often contains information on others, in our case: personalities of whistleblowers;
- carelessness as negligence and lack of professionalism. If we are in charge of this kind of information, we must be aware that we are responsible for the security of the whistleblower. Heads of organisations often think that it is more important to learn the source of information than to react on the violation, which has been revealed. It is possible that in reality, they are afraid because their own actions have involved mutual deals for the purpose of achieving materialistic goals, so-called compromises;
- conscious action. There is no secret that the point of view that everything or almost everything, including information, can be bought today, starts to dominate in the contemporary society. Information is being used as a commodity or an item of exchange. One can always find people who will wish to buy information with a far-reaching goal to protect himself or herself against any possible future threats coming from a whistleblower. Another reason for information leakage can be related to various clashes between views on politics, religion or ethnic issues.

2. There is a view that whistleblowing is a shameful activity.
   When asking a question on the reasons of failure to report, one can often receive a counter-question on what would be an opinion of other people or whether such reporting is ethical. Here we yet again encounter the issue of securing anonymity and education of public on its rights and obligations. Fighting against evil is an individual opportunity and a right of every person.
3. There is a view that it is better to keep silent and that reporting on violations is not an obligation and that it is even not a right. At the same time is taking care of one's future and fighting the evil the obligation of all other people for the sake of the one who keeps silent and could look at future with an increased security? As they say, it is none of my business, since it does not affect me. But what will happen if the evil reaches the person who had chosen to remain silent and the rest around him/her had also chosen to be the silent ones?
4. The lack of understanding of the importance of the non-disclosed information.
   Education of public on these issues has to start already at school by explaining the essence of evil and how and when it can manifest itself if someone remains silent. Explaining what can be lost.
5. The lack of feedback.
   Each person wants to know what will happen after he/she has "blown a whistle". How, what and when will something change. It is desirable that within the range of possibilities, an organisation or its sub-structure, which receives an alarm signal, informs the particular whistleblower on future actions or informs on receiving the said information and expresses thanks to the whistleblower.

3.2. Five reasons why a whistleblower provides information

1. Trust in the receiver of his/her report. A whistleblower acts in good faith that the information provided will be used according to those goals which initiated whistleblower's decision to report.
2. Realisation of one's responsibility for the country and one's own future. A whistleblower is morally and ethically motivated to participate in the fight against evil.
3. A person has not understood a particular situation and believes that it is preferable to report several times because he/she wishes to maintain good relations (may be useful in future). Perhaps a whistleblower has not understood the contents or goals or even the process? In this case, the authorities must provide feedback and explanation in order to dissipate any doubts that may have occurred. The receiver of information must show empathy. There can be situations when a whistleblower is afraid or does not believe in the process and may choose to remain silent in future. Education and encouragement must be provided.
4. Reporting and possibly willing to hide one's own violation or those of people close to him/her. A rather widespread method. By providing information on negative actions of another person, a whistleblower may mistakenly hope that he/she would be able to evade attention and responsibility.
5. Deliberately providing smearing information in order to take revenge on someone or create that person short-term unpleasant surprises.

Therefore, in order to understand the concordance of received information with a certain situation and to assess the provider of information, it is advisable to understand the motivation of the whistleblower. One can often come across situations when taking a revenge on an innocent person for some personal failures, a whistleblower slanders them without even thinking about the consequences of further events.

In this regard, the deportations of March 1949 when 42,149 people were deported from Latvia stand as a vivid example. Some forty years later a fraction of those who initiated and conducted deportations, just like during a confession, told everyone about their role in this crime.

The lists of those to be deported were prepared by the neighbours and co-workers of the soon-to-be be victims. It was unimaginably hard to listen to the reasons they gave to substantiate their actions. There were people who took revenge on someone just because their former beloved had turned them down and had chosen a different life partner. Others desired to get hold of the property of would be deportees, like furniture, agricultural machinery or just timber products, which a neighbour had obtained honestly and had intended to use for home repairs or construction. Some others had hoped to expand their living space or get a promotion. Nobody could give a positive reply when asked if such denunciations made them happy. The respondents tried to avert their eyes, full of despair and pain and stared at the ground.

4. The development of whistleblower activities in Europe

4.1. The study by Transparency International

Transparency International is an international non-governmental organisation, founded in 1993, which fights against corruption and attempts to attract public attention to the corruption-related issues.

The report on the study made by Transparency International recognises that the implementation of regulations for the protection of whistleblowers reporting on the cases of corruption in various organisations has failed in the majority of the EU member states.

Whistleblowers play an important part in the prevention and decreasing of corruption, but only four member states of the EU: Luxembourg, Romania, Slovenia and the UK have applied a respective domestic legal regulation which is in line with the recommendations of the new report. It is only in those four countries that an employee of the public or private sector organisation is adequately protected against threats and intimidation in cases of revealing serious violations of corruptive nature at his/her place of work.

Of the remaining 23 EU countries in the study, 16 partially protect employees who report wrongdoing, while seven have either no or very inadequate laws in place yet.

“Whistleblowers are very important to the fight against corruption. They take on risks that many, if not most, people are unwilling to assume and they expose crimes that few are interested in or brave enough to report,” said Anne Koch, Regional Director for Europe and Central Asia at Transparency International.

The report “Whistleblowers in Europe” was created for the purpose of contributing to the global understanding of the issue and in order to protect the interests and legal rights of whistleblowers as well as to contribute to the prevention of corruption. Transparency International has promoted and participated in the establishment, development, improvement of the legal regulatory framework for whistleblowers by committing its proposals and providing assessment in dozens of countries around the world.[286]

[286] TI publishes its report “Whistleblowing in Europe”. Acquired from http://delna.lv/lv/2013/11/06/ti-publice-zinojumu-trauksmes-celaji-eiropa/

Transparency International strongly defends the idea that the EU countries must continue to develop and implement a legal framework for whistleblowers based on international standards, including those standards that have been developed by Transparency International itself. Governments and companies should provide support to whistleblowers, particularly, in cases when violations and legal irregularities have been identified and revealed. Without robust legal regulation and a secure information procedure for the reporting of illegal activities and irregular activities in the private and public sectors, employees across Europe, as soon as they try to reveal corruption or other crimes, will continue to be at risk of being intimidated and facing threats or attempts of blackmail.

Without such regulation, the biggest corruption scandals and car crashes and other types of vengeful acts linked with them have taken lives of many people in Europe and have put their toll in financial resources. All of this could theoretically be avoided if employees enjoyed the required degree of protection.

The wording of several laws has been written in an obscure manner and contains a multitude of exemptions and legal deficiencies. Laws lack provisions on the availability of channels of openness for whistleblowers, a comprehensible definition of a whistleblower, guarantees of confidentiality and protection against defamation cases in court.

4.2. Protection of whistleblowers

Since late 20th century whistleblowing is becoming increasingly topical in Europe as well as globally. With the collapse of a large state system represented by the USSR and with the fall of the "Iron Curtain", it was mostly Europe and the USA that faced substantial immigration from the former Soviet Union and the consequences which those people brought along. The newly arrived people from the former USSR were surprisingly active at engaging in criminal activities, which in the receiving Western countries created substantial changes in everyday workload of the police and led to the reassessment of some regulations on maintaining law and order.

Changes in the legislation affected also the views of societies themselves and members of public willingly shared their observations with the police. Initially, the public addressed the issues of corruption, but later this information became useful also for solving of other crimes. The belief that whistleblowing on violations represented a democratic and responsible activity, became increasingly strong in the European public perception.

The protection of whistleblowers has been fixed in international legal acts and is a priority in such international organisations as the Council of Europe and Organisation for Economic Cooperation and Development (OECD), where Latvia is a member state.

The 1999 Civil Law Convention on Corruption of the Council of Europe as well as the 2003 UN Convention against Corruption call upon the member states to ensure due protection against negative consequences for those who have reported about instances of corruption. In 2014 the Council of Europe adopted a recommendation to its member states CM/Rec (2014)7 on "The Protection of Whistleblowers", which establishes common principles for the development of national regulation (for instance, how to define whistleblowing, recommendations on where to submit whistleblower's report, ensuring of anonymity and protection against negative consequences). The recommendation of the Council of Europe stresses that protection of persons who report on violations of public importance will promote openness and responsibility, which is so vital to democracy. On 1 June 2016 Latvia became a member state of OECD. For OECD the protection of whistleblowers is one of the horizontal priorities in the areas of fighting corruption, public administration and corporate management. The requirement to provide whistleblowing channels and protection is included in the legal instruments of OECD, studies on good governance in OECD member states have been conducted as well and OECD countries share common principles for the development of legal regulations for the protection of whistleblowers (for instance, they must include both: the state administration and the private sector, the allotment burden falls to the employer, protection must be provided to the ones who have reported and to the competent authorities). And finally, during the process of joining OECD Latvia received recommendations on the necessity to provide whistleblower protection and on the formation of channels of reporting in the private sector as well as in the state administration.[287]

The EU requirements in the area of financial and capital market have been taken into account in drafting the law. Latvia must incorporate in its national normative acts the requirements of the Directive 2015/2392 of the European Commission of 17 December 2015 on the reporting on infringements of the so-called market abuse regulations. This directive is already partially introduced by means of normative regulations of the Financial and Capital Market Commission. However, it is necessary to strengthen the protection of whistleblowers, particularly the protection of their anonymity by means of a broader comprehensive legal act, which is represented by the forthcoming specialised law.

[287] The creation of whisleblower protection mechanism in Latvia. Acquired from https://www.mk.gov.lv/sites/default/files/attachments/vkviedoklraksts_trauksmes_celeji_1.pdf

The number of countries where specialised whistleblower protection laws are under development is steadily increasing. Over the past four years, such specialised laws have entered into force in Belgium, Ireland, Slovakia, the Netherlands, and France and on 1 January 2017 – in Sweden. In Estonia, the protection of whistleblowers has been established in the Anti-Corruption Law. The law was amended in 2016 on the basis of OECD recommendation, establishing that protection shall be applied not only to whistleblowers in the state administration but also in the private sector. In Lithuania, the draft law was submitted to Seimas (parliament) in 2010, but it has not been adopted yet. For instance, on Panama documents (on the use of offshore companies) and "LuxLeaks" (on tax evasion) scandals. Thanks to whistleblowers, information on internationally important cases in respect of tax evasion has been revealed. These scandals created broad public response. At the same time, they also revealed the important role, which can be played by whistleblowers, who in the interests of public raise alarm regarding the developments at the place of their employment. These cases also showed that it is important that the national regulation establishes due protection of whistleblowers, ensuring that those persons remain anonymous, that they are protected against their employers while simultaneously not avoiding the risk of facing the court themselves. In June 2016 two former employees of "Pricewaterhouse Coopers" who were whistleblowers in the "LuxLeaks" were declared guilty by the court of first instance in Luxembourg on charges of theft, disclosure of commercial secrets as well as fraud and sentenced conditionally to imprisonment and a fine.[288]

[288] The creation of whisleblower protection mechanism in Latvia. Acquired on 10.04.2018 from https://www.mk.gov.lv/sites/default/files/attachments/vkviedoklraksts_trauksmes_celeji_1.pdf

This leads to a conclusion that the developmental activities in the fight against corruption and economic crimes in the EU countries is targeted at raising the well-being of people and the development of democracy.

Conclusions

There is a popular yet true joke in psychology: a child must be nurtured and taught while he/she can still be placed across the bed. If the child starts to sleep in a bed in a longitudinal manner, it becomes more difficult to nurture and teach him/her. We teach the next generation by our own example – an example of how to act in one or another situation, how to make decisions and take responsibility for them. Our words and deeds have an unspeakably big and a substantially lasting impact and the role basic value formation on the world-view of our children, on their understanding and sense of shared responsibility for the heritage due to be left to their own children and grandchildren, the next generations.

We are responsible for ourselves, for our children and the next generations, but our indifference, idleness, the lack of courage and even the lack of courage limits our ability to take action against a dishonest activity. Thus, we allow and very often even promote the activities or inactivity of various dishonest persons. When developing the systems of security and internal control of organisations, it is a fundamental necessity to promote the prevention and combating of bribery, money laundering as well as to diminish the shadow economy and other illegal activities, like terrorism. The state does not produce money and does not earn it. It is our own taxpayer money. We all know cases when this money is misused, mismanaged or simply stolen all too well. In situations like these, it gets into the hands of criminals. It does not get into our own hands, the hands of our children and senior citizens who are our fathers and mothers.

Perhaps "The Divine Comedy" by Dante Alighieri should be introduced in our schools as a mandatory subject?

None of us knows what is beyond that Gate!

References

Autoru kolektīvs. (2005). *Ilustrētā svešvārdu vārdnīca*. Rīga: Avots

Bojārs J. (2002). *Politiskās stratēģijas māksla un demokrātija*. Rīga: Zvaigzne ABC

Hefe O. (2009). *Taisnīgums, filosofisks ievads*. Rīga: Zvaigzne ABC

Kačevska I. (2001). *Zinātnes un tehnoloģijas vārdnīca*. Rīga: Norden AB.

Klišāne J. (1998). *Senā Grieķija*. Rīga: Zvaigzne ABC.

Kūle M, Kūlis. R. (1996). *Filosofija*. Rīga; Burtnieks

Riekstiņš. K. (2004). K*as ir septiņi nāves grēki un atbildes uz vēl 53 erudīcijas jautājumiem*. Rīga: Avots

Rubenis A. (1998). *Senās Grieķijas kultūra*. Rīga: Zvaigzne ABC

The Law on Official Publications and Legal Information. Adopted on 31.05.2012. *Latvijas Vēstnesis*, No. 96 (4699), 20.06.2012. Latest amendments 10.12.2016.

Administrative Violations Code of Latvia. Adopted on: 07.12.1984. *Ziņotājs*, No. 51, 20.12.1984. Latest amendments 04.07.2018

Law on the Protection of Whistleblowers, draft, reviewed and promulgated on 17.12.2015, MK 07.03.2017, acquired from http://tap.mk.gov.lv/lv/mk/tap/?pid=40377799&mode=mkk&date=2017-02-06

Explanatory memorandum of the Cabinet of Ministers, Law on the Protection of Whistleblowers, draft. Acquired from https://webcache.googleusercontent.com/search?q=cache:PBo7yM_PDeIJ:https://www.mk.gov.lv/lv/content/trauksmes-celeji+&cd=1&hl=lv&ct=clnk&gl=lv

The creation of whistleblower protection mechanism in Latvia. Acquired from https://www.mk.gov.lv/sites/default/files/attachments/vkviedoklraksts_trauksmes_celeji_1.pdf

The course of development the specialised legal regulation on whistleblowing. Acquired from https://www.mk.gov.lv/lv/content/trauksmes-celeji

Thatcher M. H. (1983). Conservative Party conference. Acquired from https://www.margaretthatcher.org/document/105454

Conference of the States Parties to the United Nations Convention against Corruption, acquired from http://www.unodc.org/documents/treaties/UNCAC/WorkingGroups/ImplementationReviewGroup/ExecutiveSummaries/V1401272e.pdf

Towards openness, responsibility and better governance: the promotion of whistleblowing, the fight against corruption, future prospects. International conference. Acquired from https://www.mk.gov.lv/sites/default/files/editor/trauksmes_celeju_konferences_programma_v1.12.pdf

Rainis – poet, playwright. Acquired from http://www.aspazijarainis.lv/par/rainis/

Korupcijas novēršanas un apkarošanas birojs. (2018). Korupcija. Acquired from https://www.knab.gov.lv/lv/education/forschools/

Pāvesta kārtējie septiņi nāves grēki. Acquired from http://www.ebaznica.lv/pavesta-kartejie-septini-naves-greki-3695/

Desmit Dieva baušļi. Acquired on 15.04.2018 from http://www.janabaznica.lv/luters/martina-lutera-lielais-katehisms/desmit-dieva-bausli/

About the Authors

Janis Veinbergs, *Bac.sc*
Bachelor of Social Sciences in Psychology. Professionalism – staff psychologist.
Specialization – psychological graphology, formation of a personality psychological portrait based on handwritten features. Government Security Service, State Economic Protection Department–Inspector. 1993–1999 Latvian republic Security Service, State President and parliament Security Service – instructor of professional training, head of antiterrorism department, head of parliament mobile security guard. 2005–2009 Information Analysis Service – Head of Department. Lecturer. 1) Riga Technical University (RTU) Faculty of Engineering Economics and Management 2001–2015. 2) School of Business Administration Turiba. The study program in the Department of Law Sciences "Security of Organizations" 2014.–
Prepared and conducted lectures and seminars: 1) Organization of goods control in customs activities; 2) Operative activity. Personnel motivation and conflict resolution; 3) Risk analysis.

Vilnis Veinbergs, *MPA*
Bachelor degree in Personnel Management Psychology and Master degree in Public Relations. Currently a doctoral student in Business Administration study program at the Turiba University.
Retired officer, Major of the National Armed Forces of the Republic of Latvia. Worked in the Security Service of the Republic of Latvia as a specialist of the personal security of the country's highest officials. Currently Head of the Internal Security Service and Director of Organisation and Individual Security study program at the Turiba University.

CRIME PREVENTION AND INVESTIGATION

Ryšardas Burda

Introduction

The head, the businessman, carrying out the activity in the conditions of market economy, tests a daily press from competitors in the struggle for new consumers, for new commodity markets, for quality of let out production and rendered services. The competition of competitors compels them to constantly take care of increasing the efficiency of production and economic and marketing activities, reducing costs, protecting their trade secrets, which, due to increased productivity and better management, ensure stable financial stability of the enterprise, which in turn determines their economic security.

The security of an enterprise

The security of an enterprise is a state of its defense against the negative influence of external and internal threats, destabilizing factors, in which the stable realization of the main commercial interests and purposes of the authorized activity is ensured.[289]

Who is interested in the company

The activities of any economic entity are mainly interested in:

1) the state;
2) competitors;
3) criminal structures;
4) his own staff.

[289] Фролова Т. А. (2005). *Экономика предприятия: конспект лекций*. Таганрог: ТРТУ, с. 15

This corresponds to the external and internal threats or risks of the enterprise.

Types of threats for organization

1. The threats from the state mainly are corruption.
2. The threats from competitors mostly are of a legal nature, less criminally.
3. The threats of criminal structures are only criminal acts.
4. Threats on the part of the personnel of an enterprise of a dual character: protection of own interests by legal and illegal measures, as well as criminal actions (theft, fraud, destruction of property).[290]

Necessary attributes to consider a person's behavior as a crime:

1) conflict with law – foreseeing the law;
2) hazard – the danger to the values of the existing society;
3) composition of the crime;
4) objective features are what is visible;
5) the subjective features are what the perpetrator has in mind.

It is necessary to prove all the required attributes; what is described in the article of the Penal Code – the composition. If at least one attribute is not proved – there is no crime composition, no responsibility.

Security issues:

1) What needs to be protected (property, information, securities, direct personnel of the firm)?

[290] Фролова Т. А. (2005). *Экономика предприятия: конспект лекций*. Таганрог: ТРТУ, с. 68

2) Who can represent a threat (criminal groups, personnel of the enterprise, state services)?
3) How can the threat be implemented (penetration into the premises from the street, use of personnel for mercenary purposes, etc.)?
4) Is the cost of protected objects and the cost of security comparable?

Exposure elements

To effectively build its security system, it is necessary to clearly define the following:

1) competitive struggle;
2) subjects of enterprise safety;
3) principles of building a security system;
4) means and methods of ensuring security;
5) formation of the Security Service;
6) the main functions of the Security Service;
7) legal basis for the activities of the Security Service, etc.

1. Criminal Investigation

Structural elements of the typical methodology for investigation of individual types of criminal offenses:

1) forensic character of a specific type of criminal offense;
2) a group of circumstances to be proved by a specific type of criminal offense;
3) peculiarities of initiation of pre-trial investigation and planning of initial pre-trial investigation actions for the type of criminal offense;

4) behavior of the investigator of a specific type of criminal offense (actions, program, algorithm) at each stage of the investigation, taking into account the circumstances;
5) peculiarities of tactics of pre-trial investigation actions and other organizational features;
6) use of special knowledge during the investigation of this type of criminal offense;
7) peculiarities of cooperation and organization of all law enforcement institutions during the investigation of this type of criminal offense. [291]

Elements of Forensic Characteristics of Criminal Offenses:

1) the subject of a criminal offense;
2) methods of committing and concealing a criminal offense;
3) peculiarities of the traces left by the offender (trace formation mechanism);
4) study situations;
5) characteristics of the personality of the offender. [292]

The research situation consists of the following elements:

1) the nature of the psychological character (relations between the investigator and the participants of the process, etc.);
2) informational nature (investigator's informativeness);
3) procedural and tactical (initiation of pre-trial investigation; collection of probative information, their sources, selection

[291] Burda R., Krikščiūnas R., Latauskienė E., Malevski H., Matulienė S. (2004). *Forensic tactics and methodology*. (Kriminalistikos taktika ir metodika). Vilnius, p. 86

[292] Goda G., Kazlauskas M., Kuconis P. (2011). *Baudžiamojo proceso teisė*. *Vadovėlis*. Vilnius, pp. 166–168

of preventive measures; execution of certain pre-trial investigation actions, etc.);

4) organizational-technical nature.

The situation of pre-trial investigation is a whole range of certain circumstances, which are defined at the time of the investigation.

Classification of the investigation situation:

1) typical and specificē;
2) situations that arise generally in the course of the investigation of the whole case;
3) situations that arise in the course of one single investigation operation;
4) conflict and non-conflict situations.[293]

A specific crime investigation methodology consists of:

1) initial actions of pre-trial investigation and other (informational, organizational and operational) actions;
2) further investigation actions.

Initial actions of the pre-trial investigation:

1) site inspection and/or site survey;
2) identifying the victim's personality and questioning;
3) clarification and survey of witnesses;
4) identification of a suspected personality and interview.

It is also recommended to apply the following coercive measures:

1) detention of a person;
2) personal examination;

[293] Team of authors (2013). *Kriminalistika. Taktika ir metodika. Vadovėlis*. Vilnius: Mykolo Romerio universitetas, pp. 441–445

3) perquisition;
4) the seizure.

The criminal investigation consists of the following steps:

1) evaluation of the report, statement on the incident, the received and collected material and the decision to initiate pre-trial investigation;
2) initial stage – performance of initial research actions; checking typical versions of a criminal offense; gathering evidence; organization of search and detention of a criminal offender; ensuring compensation for damage caused; setting the conditions for committing a criminal offense;
3) the next stage – other actions of the pre-trial investigation are performed, collecting, examining and evaluating the evidence (data);
4) final – completion of criminal investigation – census of accused conclusion.[294]

By providing initial pre-trial investigation, criminal intelligence and search tools, the research methodology provides more typical actions for this category of cases, recommends a series of their implementation and tactics. Depending on the nature of the investigated activity and the specific circumstances of the case, the list of primary pre-trial investigation and other actions and process of coercive measures may change.

[294] Burda R., Krikščiūnas R., Latauskienė E., Malevski H., Matulienė S. (2004). *Forensic tactics and methodology*. (Kriminalistikos taktika ir metodika). Vilnius, pp. 78–83

2. Crime prevention

Prevention is a word derived from the Latin "*pre-ventio*", which means pre-emptive pathways, eye-catching, so the word prevention means prevention, avoidance of a particular adverse event, process, and action.[295] Prevention is often accompanied by activities aimed at reducing criminal offenses. Such preventive actions of this kind are made after the commission of a criminal offense.

Prevention of violations of law is understood to have an effect not only on criminal offenses, but also on other types of legal proceeds of crime, illegal species and their determinants. These may include administrative violations, disciplinary offenses, civil legal violations, violations of procedural law.

Social prevention is understood as an extensive complex of measures aimed at influencing not only criminal offenses and other violations of law, but also all social pathologies, various determinants of behavior that deviates from social norms. These include drunkenness, drug addiction, toxicomania, suicide, prostitution, political and religious extremism, which violate not only the law but also morality, morals and other social norms.

Crime prevention is understood as a multi-level system of various interrelated state and social measures aimed at identifying, weakening and neutralizing the determinants affecting crime in order to reduce crime in the perspective of a society's development.[296]

Prevention of crime as a system, specific prevention objects, basic levels and forms, preventive measures and actors involved.

[295] Burda R., Krikščiūnas R., Latauskienė E., Malevski H., Matulienė S. (2004). *Forensic tactics and methodology*. (Kriminalistikos taktika ir metodika). Vilnius, p. 336

[296] Galinaitytė J. (2009). *Criminology: Theory and current affairs. Studio*. (Kriminologija: teorija ir aktualijos. Studija.), Vilnius, pp. 167–168

Depending on the hierarchy of crime determinants, crime science allocates these levels and types of crime prevention. Some scholars argue that there are two levels:

1) social, which combines a set of general, non-specific measures indirectly influencing crime determinants;
2) a special criminologist who is directly focused on crime determinants. The special criminological level is further divided into species:
    - general prevention aimed at the micro-environment of criminal behavior. This is non-personalized, non-personally-minded prevention;
    - individual prevention, the object of which is a person who can commit a criminal offense.[297]

The social level of crime prevention is the system used by the state, the society and all their institutes to realize their anti-criminal potential. It is a global solution to political, economic, social, and other problems in society. Therefore, social prevention measures are wide-ranging. A preventive effect is obtained in the event of a successful social and economic policy.

A specific criminological crime prevention level includes a system of measures aimed directly at identifying, weakening and neutralizing crime determinants associated with individual types of crime.

Individual prevention is understood as the educational effect on individuals, of which behavior can be anticipated in the future that they can commit a criminal offense. Depending on the personality

[297] Galinaitytė J. (2009). *Criminology: Theory and current affairs. Studio*. (Kriminologija: teorija ir aktualijos. Studija.), Vilnius, p. 173

of the offender, the individual prevention of criminal acts can be of four types and applies to the following individuals:

1) various non-criminal offenders;
2) persons who have already committed a criminal offense or who intend to do so;
3) persons who have committed a criminal offense and convicted in various penalties. The purpose of this kind of prevention is to change the provisions of convicted persons, systems of values;
4) persons sentenced to death. In this case, the purpose is to prevent recurrence.

Conclusions

1. First of all, it should be noted that the company's security is an assessment of internal and external threats.
2. One of the most important aspects of ensuring the company's security is crime investigation and crime prevention.
3. The investigation of crimes depends on the circumstances and the circumstances in which the crime is committed. An offense can be committed within the company itself – the employee himself. Misery can be committed by people from outside. It may be representatives of criminal structures, it may be competitors, or it may not be associated with competitors or criminal structures.
4. Crime prevention is relevant for every company. Prevention can be general or individual. In the company, it is often necessary to ensure a common level of security and work individually with company employees.

References

Burda R., Krikščiūnas R., Latauskienė E., Malevski H., Matulienė S. (2004). *Forensic tactics and methodology* (Kriminalistikos taktika ir metodika). Vilnius

Conklin, John E. (2004). *Criminology,* 8th ed. Boston: Pearson

Dobryninas A., Gaidys V. (2004). Is it safe for Lithuanian society? (Experience of victimisation of Lithuanian population and attitudes to criminal justice and public Safety) – the Republic of Lithuania, the Seimas of the United Nations Development Programme. (Ar saugi Lietuvos visuomenė? (Lietuvos gyventojų viktimizacijos patirtis ir požiūris į baudžiamąją justiciją bei visuomenės saugumą) – Lietuvos Respublikos, Seimas Jungtinių Tautų vystymo programa.), Vilnius

ed. Miller J. M., Wright R. A. (2005). *Encyclopedia of Criminology – Fitzroy Dearborn*

Galinaitytė J. (2009). *Criminology: Theory and current affairs. Studio* (Kriminologija: teorija ir aktualijos. Studija.), Vilnius

Goda G., Kazlauskas M., Kuconis P. (2011). *Baudžiamojo proceso teisė. Vadovėlis*. Vilnius

Shannon L. W., McKim J. L., Curry J. P., Haffner L. J. (1989). *Criminal career continuity: It's social context*. New York

Team of authors (2013). *Kriminalistika. Taktika ir metodika. Vadovėlis*. Vilnius: Mykolo Romerio universitetas

Team of autors (2010). *Crime threats and human security* (Nusikalstamumo grėsmės ir žmogaus saugumas). Mykolo Romerio universiteto Leidybos centras. Vilnius

Фролова Т. А. (2005). *Экономика предприятия: конспект лекций*. Таганрог: ТРТУ

About the Author

Rysardas Burda, *Dr. professor*, General Staff Officer
Dr. Rysardas Burda is a professor at the Faculty of Law at the University of Kazimieras Simonavičius, working in a key position. Prepared study program "Law and economic security".
He teaches at the University Bachelor's and Master's Degree Programs the following subjects: criminal procedure law, Criminology, Personal and property law protection, Economic crime investigation

Part IV

Training on security

METHODS OF STUDYING SECURITY

Harri Ruoslahti

Introduction

Security management has risen towards an independent field of study during the past decades. The field is however quite broad, from corporate continuity, cybersecurity, through crisis management, international affairs, to national security and resilience. One noticeable trend is that many modern security related solutions include a lot of technology, and can be considered cyber-physical systems, which include four domains: 1) physical (system components), 2) information (data and software), 3) cognitive (user), and 4) social (user networks). These domains should be taken into account, when studying the field of security, or developing applied security solutions.

Different professions are based on a body of knowledge and have recommended practices. Formal definitions are applied when developing education and research programs.[298] Studies in the field of security management can draw their methodology from various fields of science, e.g. systems sciences, social sciences, psychology, and even very applied approaches like engineering[299] or service design methods.[300] Co-creative methods help include the views of different

[298] Zabasta A., Carreira P., Nikiforova O., Amaral V., Kunicina N., Goulão M, … Sukovskis, L. (2017). Developing a mutually-recognized cross-domain study program in cyber-physical systems. *IEEE Global Engineering Education Conference (EDUCON)*, pp. 791–799

[299] Rajamäki J. & Ruoslahti H. (2018). Educational Competences with regard to Critical Infrastructure Protection, submitted to *17th Conference on Cyber Warfare and Security – ECCWS*, June 28th–29th, Olso, Norway

[300] Ojasalo, K., & Ojasalo, J. (2015). Adapting Business Model Thinking to Service Logic: an Empirical Study on Developing a Service Design Tool, Service Marketing and Management for the Future, CERS, Hanken School of Economics, pp. 309–333

interest groups, industry, academia, and especially end-users, to create new knowledge and innovation.[301] Within these end-user organizations, there are different interest groups, who should be included; operative practitioners, technology experts, and decision/ policy-makers should be listened to.[302] The field of security is very much applied research, which even ranges to the direct development of security related solutions and services. Thus a wide range of research and development methods are needed.

This paper is an overview of some of the methodology for the field of security. It looks at a wide range of research methods available for applied research (quantitative and qualitative), and development (engineering and service design) methods.

Including a wide range of end-user and industry representatives, as well as academics and students (class or thesis work) in a co-creative manner to question and analyse existing practices, and modelling and exploring, and testing possible services solutions can provide new knowledge.[303] Enquiry of the field of security could, for

[301] Ruoslahti, H. (2018). Co-creation of Knowledge for Innovation and Multi-Stakeholder Participation of End Users*: A Structured Literature Review*. Proceedings of EUPRERA 2017, in press;

Pirinen, R. (2015). Studies of Externally Funded Research and Development Projects in Higher Education: *Knowledge Sources and Transfers, Creative Education*, 2015, 6, 3, pp. 315–330, Scientific Research Publishing, Irvine, United States

[302] Ruoslahti H., & Knuuttila J. (2011). Listen to three types of border guard – adopting technology into the process of border checks. *Credibility Assessment and Screening Technologies at the 45th Hawaii International Conference of Systems Sciences*

[303] Rajamäki, J. & Ruoslahti, H. (2018). Educational Competences with regard to Critical Infrastructure Protection, submitted to 17th *Conference on Cyber Warfare and Security – ECCWS*, June 28th–29th, Olso, Norway;

Ruoslahti, H., & Tikanmäki, I. (2017). End-Users Co-create Shared Information for a More Complete Real-time Maritime Picture. *Proceedings of the 9th International Joint Conference on Knowledge Discovery, Knowledge Engineering and Knowledge Management*, Volume 3, pp. 267–274;

Pirinen, R. (2017). Resilient Learning: Towards Integration of Strategic Research Programmes*, International Journal of Engineering Pedagogy*, No. 7(2), pp. 94–108 example follow the Nonaka & Takeuchi (1995) Knowledge Creation Model to support innovations, or the Expansive Learning Process by Engeström, et al. (2007). The Expansive Learning Process is cyclical and has seven phases, which begin with 1) questioning existing practices, followed by 2) analysing existing practices, 3) modelling a new solution, 4) and exploring a new solution, which lead to 5) adopting this new solution, and 6) evaluating the process, to finally 7) solidify and expand new practices.

The innovative use of methods and elements from a wide range of disciplines are available for the research design. Also, co-creative methods include the views of multiple actors to create new knowledge and innovation. In this, representation of the various interest groups that end-user organizations have should be included. Security management exists to support society, its functions and businesses. The aims for security research, thus must draw from the strategy of whom it supports. On a corporate level the company strategy, on a national level the programs for internal or homeland security, and on an EU-level funding programs such as the Horizon 2020 Security Calls pave the way for identifying relevant research and development problems.

1. Security studies in Literature

1.1. Researching Security

Security studies emerged, as a scientific field, after the Second World War, as a sub-discipline under international affairs and military science. The field has become interdisciplinary as it combines methods of several disciplines in mainly analysing "links between security, culture and the identity of individuals and societies".[304]

[304] Szpyra, R. (2014). Military Security within the Framework of Security Studies: Research Results. *Garmisch-Partenkirchen*, Vol. 13, Iss. 3, p. 60

One main focus within the enquiry of security are the technological solutions to security related problems, also including thorough checks for relevant social, ethical,[305] and legislative issues. This trend has been demonstrated in the many publicly funded EU FP-7 and Horizon 2020 Security (SEC) programmes that have called for technological innovation and harmonization, resulting in projects such as AIRBEAM, ABC4EU, EUCISE 2020, GAP, IECEU, MARISA, and PERSEUS, in which Laurea University of Applied Sciences has been an active partner.

In the social sciences security can be seen "as the certainty of the existence and survival as well as the functioning and development of the subject."[306] Vos (2017, p. 4) sees that resilience is the basis for the long-term viability of organisations, and as such it is about coping with change and unexpected events. To achieve security in the face of threats one should 1) obtain situational awareness; and 2) neutralize possible threats; 3) to maintain continuity; 4) as threats are prevent achieving desired levels of security. Organisational resilience in facing disruptive events entails understanding issues, reducing (complex and interrelated) risks, and mitigating resulting crises.[307] Siedschlag offers scenario-based foresight as a forward thinking method to increase the ability to cope with possible alternative futures. Within the relatively new field of security research the notion of security is essentially linked to society. Security should be seen as a process, not a state.[308]

[305] Siedschlag, A. (2013). *Information & Security*; Sofia, Vol. 29, Iss. 1: pp. 5–17

[306] Szpyra, R. (2014). Military Security within the Framework of Security Studies: Research Results. *Garmisch-Partenkirchen,* Vol. 13, Iss. 3, (Summer 2014): p. 61

[307] Vos, M. (2017). *Communication in Turbulent Times: Exploring Issue Arenas and Crisis Communication to Enhance Organisational Resilience*, Jyväskylä University School of Business and Economics, No. 40 / 2017

[308] Siedschlag, A. (2013). *Information & Security*; Sofia, Vol. 29, Iss. 1: pp. 5–17

1.2. Resilience and Continuity

Resilience can be seen as a comprehensive and multidisciplinary approach to cope with change and manage the unexpected.[309] Linkov, et al. (2013) see resilience as a network property, and note that despite careful planning and preparation, threats may not even be recognized until they manifest.[310] Zhang writes "crises cannot be completely prevented, which calls for organisational resilience".[311] Organisations should be able to maintain themselves under challenging conditions, such as adversity, strain or barriers. Organisational resilience deals with maintaining continuity of operations to achieve organisational goals. Continuity is also in the centre for corporate security according to the Confederation of Finnish Industries (2018).

To be resilient, systems that provide critical services (for example, project networks or organisations) need to maintain four abilities. They should be able to 1) plan/prepare, 2) absorb, 3) recover, and 4) adapt to known and unknown threats.[312] Crises are not only negative events, but they may also improve organisational learning.[313]

[309] Robert, B., Morabito, L., Cloutier, I. and Hémond, Y. (2015). Interdependent critical infrastructures resilience: Methodology and case study, *Disaster Prevention and Management*, Vol. 24 No. 1, pp. 70–79

[310] Linkov, I., Eisenberg, D. A., Plourde, K., Seager, T. P., Allen, J., & Kott, A. (2013). Resilience metrics for cyber systems. *Environment Systems and Decisions*, No. 33(4), pp. 471–476

[311] Zhang, B. (2017). *Understanding Evolving Organisational Issues in Social Media*. Jyväskylä Studies in Humanities 316, Jyväskylä University Printing House, Jyväskylä, p. 25

[312] The National Academy of Sciences, NAS (2012). Linkov, I., Eisenberg, D. A., Plourde, K., Seager, T. P., Allen, J., & Kott, A. (2013). Resilience metrics for cyber systems. *Environment Systems and Decisions*, No. 33(4)

[313] Zhang, B. (2017). *Understanding Evolving Organisational Issues in Social Media*. Jyväskylä Studies in Humanities 316, Jyväskylä University Printing House, Jyväskylä

Linkov, I., Eisenberg, D. A., Plourde, K., Seager, T. P., Allen, J., & Kott, A. (2013). Resilience metrics for cyber systems. *Environment Systems and Decisions*, No. 33(4)

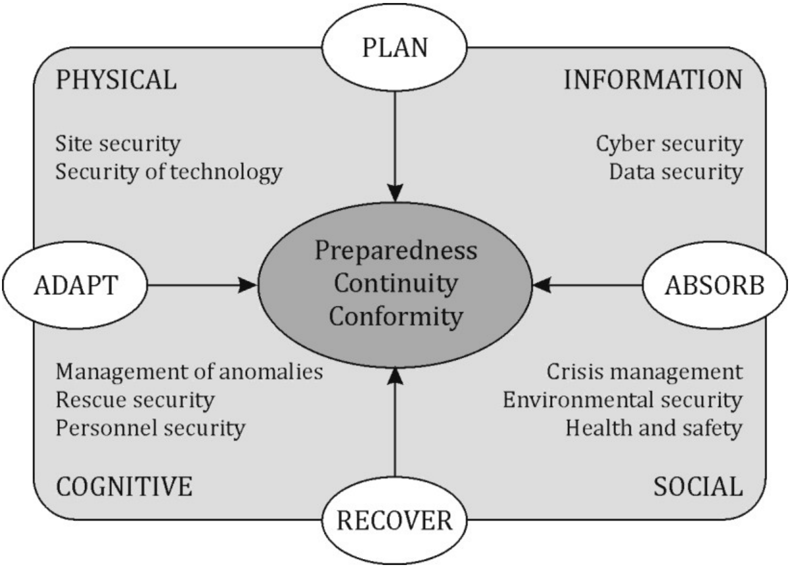


Figure 1. **A framework of the field of security**
(based on Confederation of Finnish Industries, 2018;
Linkov, 2013; 2012; Pirinen, 2017)

The above framework (Figure 1) of the field of security demonstrates that being prepared to maintain continuity, and conforming to regulations are in the focus of resilient security. It combines elements of the Confederation of Finnish Industries (2018) security management framework, and Linkov et al. (2013) who offer a metrics framework (Table 1) that combines domains for shared situational awareness and decentralized decision-making: 1) physical, 2) information, 3) cognitive, 4) social. Resilience of a cyber-physical system depends on all aspects of an organization functioning effectively throughout the four domains of the event management cycle 1) plan/prepare, 2) absorb, 3) recover, and 4) adapt.

Rajamäki & Pirinen offer three networks included in CPS systems: 1) platform, 2) software and 3) social network. Resilient networks offer continuity of information sharing between the different stakeholders of the social network, on the platform, and via layers of software. Trust should be systematically built on all these layers.[314]

As the solutions researched in the field of security studies are increasingly cyber-physical systems (CPS), the focus of CPS education should thus also focus on cooperation and information sharing between different stakeholders. This is the way to promote more resilient complex systems of systems. Students need frameworks and models that enable resilience and country management across the entire network to maintain and improve critical functionalities.[315]

Ruggiero notes that planning processes contribute to organisational preparedness for crises. Preparedness and planning are often dominant in crisis management.[316] However crisis teams also need "skills for improvisation, creative problem solving and flexibility to act in the face of the unknown", which skills can be rehearsed during crisis training and exercises, and promoted by management.[317]

[314] Rajamäki, J., & Pirinen, R. (2015). Critical infrastructure protection: towards a design theory for resilient software-intensive systems. In Proceedings of the *European Intelligence and Security Informatics Conference (EISIC)*, IEEE Conference Publications

[315] Rajamäki, J. & Ruoslahti, H. (2018). Educational Competences with regard to Critical Infrastructure Protection, submitted to *17th Conference on Cyber Warfare and Security – ECCWS*, June 28th–29th, Olso, Norway

[316] Ruggiero, A. (2017). *Crisis Communication and Terrorism: Mapping Challenges and Co-creating Solutions*. Jyväskylä Studies in Humanities 324, Jyväskylä University Printing House, Jyväskylä 2017

[317] Salokannel, J., Knuuttila, J., & Ruoslahti, H. (2015). Arctic Maritime Safety and Security – the Human Element seen from the Captain´s Table, presented at *International Conference on Safe and Sustainable Shipping in a Changing Arctic Environment*, ShipArc 2015, August 25th–27 th, 2015, Malmö Sweden, in press for proceedings. p. 25

Organisations should simultaneously prepare for a variety of hazards, as crises share commonalities, calling for common response patterns and general preparedness planning and training.[318] Different response strategies can be chosen to respond to crises that threaten organizational continuity, "complex evolving crises may require adjustment and multiple solutions". [319] Trust within social networks quantifies the information shared, and identifies with whom.[320]

1.3. Managing Crisis

Crisis, triggered by incidents or occurring risks may have negative consequences, such as damage to organisational reputation or financial losses, for example.[321] No one alone can fully control complex integrated cyber-physical systems, for this reason coordination and cooperation are needed.[322] One key in handling crisis and recovering from disturbances is open and clear information exchange. Higher education competences in resilience should address both theory and practical skills in communication, building interoperability between organizations, and understanding how to build and

[318] Ruggiero, A. (2017). *Crisis Communication and Terrorism: Mapping Challenges and Co-creating Solutions*. Jyväskylä Studies in Humanities 324, Jyväskylä University Printing House, Jyväskylä 2017

[319] Zhang, B. (2017). *Understanding Evolving Organisational Issues in Social Media*. Jyväskylä Studies in Humanities 316, Jyväskylä University Printing House, Jyväskylä p. 26

[320] Rajamäki, J. & Ruoslahti, H. (2018). Educational Competences with regard to Critical Infrastructure Protection, submitted to *17th Conference on Cyber Warfare and Security – ECCWS*, June 28th–29th, Olso, Norway

[321] Zhang, B. (2017). *Understanding Evolving Organisational Issues in Social Media*

[322] Rajamäki, J. & Ruoslahti, H. (2018). Educational Competences with regard to Critical Infrastructure Protection, submitted to *17th Conference on Cyber Warfare and Security – ECCWS*, June 28th–29th, Olso, Norway

maintain shared situational awareness. These all are needed to effectively respond to disturbances and collaborate effectively.[323]

Crisis constitute disruptions in the everyday operations.[324] This is why, when we anticipate and prepare for possible crisis, communication about them becomes an ongoing process.[325] Reynolds & Seeger offer the Crisis and Emergency Risk Communication Model (CERC) that focusses on the crisis communication process and offers five phases: 1) pre-crisis; 2) initial event; 3) maintenance; 4) resolution; and 5) evaluation.[326]

These five phases could, for example, be combined with the three CPS networks by Rajamäki and Pirinen (2015) to provide one possible analysis framework (Table 2) to make sense of communication within CPSs during crisis.

[323] Rajamäki, J. & Ruoslahti, H. (2018). Educational Competences with regard to Critical Infrastructure Protection, submitted to *17th Conference on Cyber Warfare and Security – ECCWS*, June 28th–29th, Olso, Norway;

Ruoslahti, H., & Tikanmäki, I. (2017). End-Users Co-create Shared Information for a More Complete Real-time Maritime Picture. Proceedings of the *9th International Joint Conference on Knowledge Discovery*, *Knowledge Engineering and Knowledge Management*, Volume 3

[324] Ruggiero, A. (2017). Crisis Communication and Terrorism: Mapping Challenges and Co-creating Solutions. *Jyväskylä Studies in Humanities,* 324, Jyväskylä University;

Linkov, I., Eisenberg, D. A., Plourde, K., Seager, T. P., Allen, J., & Kott, A. (2013). Resilience metrics for cyber systems. *Environment Systems and Decisions*, No. 33(4), pp. 471–476, kylä 2017

[325] Ruggiero, A. (2017). Crisis Communication and Terrorism: Mapping Challenges and Co-creating Solutions. *Jyväskylä Studies in Humanities,* 324, Jyväskylä University;

Vos, M. (2017). Communication in Turbulent Times: Exploring Issue Arenas and Crisis Communication to Enhance Organisational Resilience, Jyväskylä University School of Business and Economics, No. 40/2017, *Printing Hou*se, Jyväs

[326] Reynolds, B. & Seeger, M. W. (2005). Crisis and emergency risk communication as an integrative model. *Journal of Health Communication*, No. 10 (1), pp. 43–55

2. Methods

2.1. Research methods used in security studies

Siedschlag offers an embedded scenario method, where scenarios for security roles are first collected; then context for roles, tasks, and missions for actors; and third, validated reference scenarios lead to a proposed roadmap for security research. These reference scenarios must respect both human and societal needs, because citizens are the ultimate end-users of security research. Security research has the duty of proposing "ways to more strongly link civil security authorities to citizenry, and citizenry to technologies".[327]

2.2. Relevance and Rigour

Research should strive to be rigorous and relevant. Hevner et al. (2005) write how research is there to develop theories or artefacts, using its different methods to justify and evaluate them. Relevance of research is tied to the (business) needs of its environment, its people, organisations, and technology. Research should take into account peoples' roles, capabilities, and characteristics. On an organisational level research is interested in strategies, structures, cultures, and processes, for example. Interesting issues in technology may be its infrastructure, applications, communications, and development capabilities. Rigor of research is based on creating new knowledge. It is founded on theories, frameworks, constructs, and models, and structured methodologies and validation criteria are used to collect, measure, analyse data.

[327] Siedschlag, A. (2013). *Information & Security*. Sofia, Vol. 29, Iss. 1: p. 8

Relevance in research research means that the work makes a practical contribution by being relevant to business and authority practitioners. The work is applied in nature research can strive to answer specific research questions or set development goals. Emphasis is put on finding practical, immediate, and relevant results that can be put to practice. Results are typically published in practitioner and industry magazines or consulting reports.

Rigorous scientific research hence means that the emphasis is on meeting scientific standards such as validity and reliability. Research work aims at theoretical contribution, and is subjected to academic peer review and published in academic journals. To meet this requirement of rigour students are encouraged to share their methods and results with one another and thesis are made public.

Two examples of analysis frameworks that take into account both relevance and rigour are presented in Tables 1 and 2. Either of these could be used to study the field of security. In fact the framework presented in Table 1 has been used by Linkov et al. (2013) as resilience metrics for cyber systems.

Table 1

Example combining the four domains for shared situational awareness and decentralized decision-making and the four domains of the event management cycle[328]

	Physical	Information	Cognitive (user)	Social
Plan/Prepare				
Absorb				
Recover				
Adapt				

[328] Linkov, I., Eisenberg, D. A., Plourde, K., Seager, T. P., Allen, J., & Kott, A. (2013). Resilience metrics for cyber systems. *Environment Systems and Decisions*, No. 33(4), pp. 471–476

Table 2

Example combining the five phases of the Crisis and Emergency Risk Communication Model[329] with the three networks of CPS[330]

	Platform Network	Software Network	Social Network
Pre-Crisis			
Initial Event			
Maintenance			
Resolution			
Evaluation			

Some commonly used research and development methods are presented in Table 3. These are divided into three main categories: quantitative research methods, qualitative research methods, and development methods.

Table 3

Examples of some commonly used research and development methods

Quantitative research Focus on numbers	**Qualitative research Focus on text**	**Development methods Focus on artefacts**
Survey	Action research	Service design
Laboratory experiment	Ethnography	Design thinking
Simulation	Content analysis	Iterative cycle
Mathematical modelling	Structured literature review	Last mile research
Statistical analysis	Semiotics	System design
Econometrics	Hermeneutics	Robust design
Case Study	Case Study	Product engineering

[329] Reynolds, B. & Seeger, M. W. (2005). Crisis and emergency risk communication as an integrative model. *Journal of Health Communication,* No. 10 (1), pp. 43–55

[330] Rajamäki, J., & Pirinen, R. (2015). Critical infrastructure protection: towards a design theory for resilient software-intensive systems. *In Proceedings of the European Intelligence and Security Informatics Conference (EISIC)*, IEEE Conference Publications

Conclusions and recommendations

First, the innovative use of methods and elements from a wide range of disciplines are available for the research design (such as in Table 2). When having a research focus there is a wide range of both qualitative and quantitative methods to choose from. The research question of the study guides the choice of research and data collection methods; or, with a development focus the development goals and expected outcome or artefacts guide the choice of method.

Second, co-creative methods include the views of multiple actors to create new knowledge and innovation. Representatives of different interest groups that end-user organizations have should be included to provide needed expertise and different points of view.

Third, security management is there to support society, its functions and businesses. Aims for security research, thus draw from the strategy of whom it supports. On a corporate level it is the company strategy, on a national level the programs for internal or homeland security, and on an EU-level programs such as the Horizon 2020 Security Calls.

Fourth, higher education should provide students with frameworks and models that enable the study of security and resilience management of critical functionalities. Students need knowledge about the innovative use of both research and development methods, research design and execution, as well as how to collaborate with stakeholders in co-creative ways, and involving different viewpoints. Students should be able to think on a strategic level, so that their projects serve the aims of the businesses, authorities, or society that their research and development activities support.

References

Engeström, Y., Kerosuo, H., & Kajamaa, A. (2007). Beyond Discontinuity: Expansive Organizational Learning Remembered, *Management Learning*, No. 38, 3, pp. 319–336, Sage Publications Ltd., Thousand Oaks, United Kingdom

Hevner, A. R., March, S. T., Park, J., Ram, S. (2004). Design Science in Information Systems Research 1, *MIS Quarterly*, Mart 28, 1; pp. 75–105

Linkov, I., Eisenberg, D. A., Plourde, K., Seager, T. P., Allen, J., & Kott, A. (2013). Resilience metrics for cyber systems. *Environment Systems and Decisions*, No. 33(4), pp. 471–476

Nonaka, I. & Takeuchi, H. (1995). *The Knowledge–Creating Company – How Japanese Companies create the dynamics of Innovation*. New York: Oxford University Press

Ojasalo, K., & Ojasalo, J. (2015). Adapting Business Model Thinking to Service Logic: an Empirical Study on Developing a Service Design Tool, *Service Marketing and Management for the Future*, CERS, Hanken School of Economics, pp. 309–333

Pirinen, R. (2017). Resilient Learning: Towards Integration of Strategic Research Programmes, *International Journal of Engineering Pedagogy*, No. 7(2), pp. 94-108

Pirinen, R. (2015). Studies of Externally Funded Research and Development Projects in Higher Education: Knowledge Sources and Transfers, *Creative Education*, No. 6, 3, pp. 315–330, Scientific Research Publishing, Irvine, United States

Rajamäki, J., & Pirinen R. (2015). Critical infrastructure protection: towards a design theory for resilient software-intensive systems. *In Proceedings of the European Intelligence and Security Informatics Conference (EISIC)*, IEEE Conference Publications

Rajamäki, J. & Ruoslahti, H. (2018). Educational Competences with regard to Critical Infrastructure Protection, submitted to *17th Conference on Cyber Warfare and Security – ECCWS*, June 28th–29th, Olso, Norway

Reynolds, B. & Seeger, M. W. (2005). Crisis and emergency risk communication as an integrative model. *Journal of Health Communication*, No. 10 (1), pp. 43–55

Robert, B., Morabito, L., Cloutier, I. and Hémond, Y. (2015). Interdependent critical infrastructures resilience: Methodology and case study, *Disaster Prevention and Management*, Vol. 24 No. 1, pp. 70–79

Ruggiero, A. (2017). Crisis Communication and Terrorism: Mapping Challenges and Co-creating Solutions. *Jyväskylä Studies in Humanities 324*, *Jyväskylä University Printing Hous*e, Jyväskylä 2017

Ruoslahti, H. (2018). Co-creation of Knowledge for Innovation and Multi–Stakeholder Participation of End Users: *A Structured Literature Review*. Proceedings of EUPRERA 2017, in press

Ruoslahti, H., & Knuuttila, J. (2011). Listen to three types of border guard – adopting technology into the process of border checks. Credibility Assessment and Screening Technologies at the 45th Hawaii International Conference of Systems Sciences

Salokannel, J., Knuuttila, J., & Ruoslahti, H. (2015). Arctic Maritime Safety and Security – the Human Element seen from the Captain´s Table, presented at International Conference on Safe and Sustainable Shipping in a Changing Arctic Environment, ShipArc 2015, August 25–27, 2015, Malmö Sweden, in press for proceedings

Ruoslahti, H., & Tikanmäki, I. (2017). End-Users Co-create Shared Information for a More Complete Real-time Maritime Picture. Proceedings of the *9th International Joint Conference on Knowledge Discovery, Knowledge Engineering and Knowledge Management*, Volume 3, pp. 267–274

Siedschlag, A. (2013). *Information & Security*. Sofia, Vol. 29, Iss. 1: pp. 5–17

Szpyra, R. (2014). Military Security within the Framework of Security Studies: Research Results. *Garmisch-Partenkirchen,* Vol. 13, Iss. 3, (Summer 2014): pp. 59–82

Vos, M. (2017). Communication in Turbulent Times: Exploring Issue Arenas and Crisis Communication to Enhance Organisational Resilience, Jyväskylä University School of Business and Economics, No. 40 / 2017

Zabasta, A., Carreira, P., Nikiforova, O., Amaral, V., Kunicina, N., Goulão, M, … Sukovskis, L. (2017). Developing a mutually-recognized cross-domain study program in cyber-physical systems. *IEEE Global Engineering Education Conference (EDUCON)*, pp. 791–799

Zhang, B. (2017). Understanding Evolving Organisational Issues in Social Media. *Jyväskylä Studies in Humanities 316*, Jyväskylä University Printing House, Jyväskylä

Confederation of Finnish Industries (2018). Retrieved from https://ek.fi/mita-teemme/tyoelama/yritysturvallisuus/

Laurea University of Applied Sciences (2018). Retrieved from https://www.laurea.fi/en/research-development-and-innovations/references

National Academy of Sciences (US) (2012). Disaster resilience: a national imperative

About the Author

Harri Ruoslahti, Master of Arts in Communication from Pepperdine University (California, USA); and is currently a PhD student focusing on co-creation in multi-stakeholder settings at the department of organizational communication at the University of Jyväskylä, Finland.

Harri Ruoslahti, Senior Lecturer at Laurea UAS Finland, divides his time teaching the Security Management Program, and working on security governance related research and innovation projects, focusing on stakeholder integration and management as part of the project network, where he has been active in scenario building, management and facilitation of expert panels, and management and evaluation of external communication. He is the co-founder of BX Border Solutions, a Finnish company offering innovative solutions for border crossing, which are based on experience in related innovation projects. He has worked prior to Laurea in executive development, and in sales. Harri began his career in the Finnish Coast Guard, and has the rank of Lieutenant Commander.

SECURITY TRAINING STANDARD AS A TOOL FOR UNIFICATION OF PROFESSIONAL COMPETENCES AND REQUIREMENTS FOR PRIVATE SECURITY EMPLOYEES

Raimundas Kalesnykas

Introduction

The ever-changing socio-economic, political and security environment poses new challenges for employees working in public and private security sectors. Member States and EU society are increasing the requirements for public and private security employees for professionalism, accountability, responsibility, publicity of their activities. Many EU countries pointed the need to continue the discussion on establishment of professional training standard for private security staff.[331] Member States aspiration – to educate and train a professional and skilled security employee, who can solve various security problems by providing security services to customers – remains a negotiable issue between the private security sector practitioners and researchers too.

[331] The new security company: integration of services and technology responding to changes in customer demand, demography and technology (Fifth White Paper, Berlin, 23 April 2015). Belgium: CoESS – Confederation of European Security Services, 52 p. Retrieved from http://www.coess.org/newsroom.php?page=white-papers

The relevance of research is linked to the changes of professional requirements for private security employees and to challenges in order of finding a standardized tool of private security employees training. Education is a key component of the effort to raise the standard of private security training yet a number of researchers have expressed concerns about the minimal training requirements of private security staff.[332] Indeed, in the Member States is no standardisation on the level of training required in order to become a private security employee. Some researchers have noted that private security personnel are less carefully screened and receive less (or poor) training that public police officers[333]. In other hand, appropriate training will determine the extent to which private security personnel are effectively able to take on the role of "para-police" in which they utilize the full legal tools at their disposal.[334]

Customers of private security services are continually increasing requirements for private security personnel, preferring professional, high quality and cost-effective security services. Private security employees require adequate training in order to ensure a satisfactory level of professionalism in the private security sector, and to guarantee that the rules and regulations on what

[332] Kalesnykas, R., Dieninis, L. (2010). The legal regulation of professional requirements for private security personnel: the experience of Lithuania and some European Union countries. *Current Issues of Business and Law*, Vol. 5, No. 1, pp. 223–241;

Button, M. (2007). Assessing the regulation of private security across Europe. *European Journal of Criminology*, Vol. 4(1), pp. 109–128;

Collins, S.C., Britto, S., Britto, M. (2008). High-school private security programs: the wave of the future? *Security Journal*, No. 21, pp. 159–172

[333] Montgomery, R., Taylor, C. (2015). *The use of private security services for policing*. Ontario, Canada: Public Safety Canada, pp. 45–46

[334] Button, M. (2008). *Doing security: critical reflections and an agenda for change*. Houndmills, UK: Palgrave Macmillan, p. 78

constitutes proper conduct in respect to providing security services. Professional competence is considered to be the most important and effective indicator of the quality of performance of private security services.

The object of research is oriented of finding common standardized requirements for private security employees' professional competence and defining the appropriate level of their training. This article encompasses *research problems* related to validation of regulatory measures of professional requirements for private security staff. Research studies and legal analysis show that the Member States have established minimum requirements (e.g., age, good health, basic training and education and lack of conviction) for persons wishing to engage in the private security activities.[335] However, many EU countries do not define and set the requirements to be applied for private security managers. The reason for this is related with the different Member States' national policies and regulatory framework of private security industry.[336]

Nowadays private security companies invest in its employees' professionalism, education and training. Member States are looking into the feasibility of private security personnel requirements in order to provide unified professional training and educational standards

[335] Button, M., Stiernstedt, P. (2018). Comparing private security regulation in the European Union. Policing and society: an *international journal of research and policy*, Vol. 28 (4), pp. 398–414

[336] Kalesnykas, R. (2002). Possibilities to integrate the private security in the system of law and order. *Jurisprudence: academic journal of Mykolas Romeris University*, No. 26 (18), pp. 71–82;

Button, M., Stiernstedt, P. (2017). The evolution of security industry regulation in the European Union. I*nternational journal of comparative and applied criminal justice*, Vol. 41 (4), pp. 245–257 and the legal conditions of their implementation. The EU sets high requirements for the private security personnel: they must have professional and higher education knowledge to meet the modern scientific and technological level as well as the necessary competence to practice and facilitate the development and updating of the previously acquired knowledge so that they are able to adapt to the constantly changing requirements in the security market. In this article is presented the importance of unification of professional competences and requirements of age and health, and recruitment of private security personnel. Issues in establishing an EU security training standard also are discussed.

1. Standardization of professional requirements for private security personnel

Member States still do not have a single regulatory framework for private security industry. Only in a few EU countries (Hungary, Slovenia, Poland, Lithuania, Estonia, Luxembourg, Belgium) the private security business is well-developed and competitive with the public security sector. In other Member States (Greece, Cyprus, Italy, Germany, Austria, France) the private security companies' activities are regulated formally, without any clear conditions for the development of private security business.[337] These various manners of looking at the private security sector have led the EU to start a discussion about adoption a unified legislation for private security companies. This has resulted in a highly diverse of private security business in the European landscape. This diversity has sometimes

[337] Kalesnykas, R., Dieninis, L. (2010). The legal regulation of professional requirements for private security personnel: the experience of Lithuania and some European Union countries. *Current Issues of Business and Law*, Vol. 5, No. 1, pp. 223–241

led to differences in how activities coming under security area are defined, in proposals for statutory frameworks, in the conditions for accessing the profession and in how to define a minimum level of training, how to organise oversight of the sector or how to manage the sensitive issues of accountability, responsibility or the use weapons.[338]

One of the most important control mechanisms of private security industry development is establishing the licensing system. Licensing for private security companies is mandatory by national law in all Members States. It determines which type of services can be provided and which requirements apply to private security companies and their employees. These requirements included a great variety of criteria. A minimum age, the absence of serious criminal offences on his or her record, identifiable insignia for personnel – a uniform and an identity badge/card – are as basic requirements for any entry level of private security companies staff. Special conditions, such as training and instruction of the use of armed force and its legal requirements, also are applied. Some particularly sensitive sectors (e.g., aviation security, maritime security, etc.) may stipulate drug screening and psychological profiling[339].

The standardization of professional requirements for private security personnel is vital to the professionalism and moral integrity of the private security sector. It is considered as an interest of the private security industry to self-regulate according to the minimum standards for the selection and recruitment of personnel, in particular

[338] Kalesnykas, R. (2005). The threat as a dimension for security industry development. *Jurisprudence: academic journal of Mykolas Romeris University*, No. 76 (68), pp. 102–112

[339] Button, M., Stiernstedt, P. (2018). Comparing private security regulation in the European Union. *Policing and society: an international journal of research and policy*, Vol. 28 (4), pp. 398–414

to avoid potential cases of liability.[340] Ongoing discussions between security experts indicated that the fact that it is difficult to establish at what age or after achieving what level of education the optimum performance of security personnel can be ensured, is a reason for the need to achieve a standardization of the minimum requirements for recruitment at the national or international level.[341] In particular, the very nature of private security work carries the danger of the unnecessary use of force by employees who may not have received adequate background screening. The legislation of professional requirements for private security personnel varies greatly across the Member States.

1.1. Requirements for the age of private security employees

All individuals wishing to enter the private security profession in the EU must meet three basic conditions: age, education and good moral character (have no criminal record). As illustrated by Table 1, the average age of a private security guard working in the EU private security industry is ±38 % and the average percentage of men active in the private security industry is ±82 % versus ±18 % for women.[342]

[340] Berg, J. (2007). The accountability of South Africa's private security industry: mechanisms of control and challenges to effective oversight. Newlands, South Africa: Criminal Justice Initiative of the Open Society Foundation for South Africa, p. 19

[341] The socio-economic added value of private security services in Europe (2013). Belgium: CoESS –Confederation of European Security Services, p. 14. Retrieved from file:///D:/Downloads/wp-4-2013-the-socio-economic-added-value-of-private-security-services-in-europe.pdf

[342] The new security company: integration of services and technology responding to changes in customer demand, demography and technology (5th White Paper, Berlin, 23 April 2015). Belgium: CoESS – Confederation of European Security Services, p. 32. Retrieved from http://www.coess.org/newsroom.php?page=white-papers;

Of course, it is necessary to point out that the age in some EU countries (Bulgaria, Germany, Ireland, Italy, Portugal, Spain, and Finland) is much higher than this average.

Table 1

Average of age and gender of private security employees

EU country	Age (years)	Male/Female (%)	EU country	Age (years)	Male/Female (%)
Austria	38	80/20	Ireland	45	95/5
Belgium	35	85/15	Italy	42	90/10
Bulgaria	45	87/13	Latvia	35	80/20
Croatia	35	88/12	Lithuania	30	80/20
Cyprus	37	75/25	Luxembourg	38	80/20
Denmark	38	80/20	the Netherlands	27	75/25
Estonia	40	80/20	Poland	38	95/5
Finland	40	75/25	Portugal	42	80/20
France	38	84/16	Romania	35	85/15
Germany	45	80/20	Slovenia	32	90/10
Greece	27	80/20	Spain	40	85/15
Hungary	36	85/15	Sweden	30	70/30
Average	*38*	*82/18*			

** Source CoESS (2013)*[343]

In most cases, age requirements for employees of private security companies are formal and usually regulated by national laws of the Member State. Most countries in the EU have established a

Private Security Services in Europe: CoESS Facts and Figures 2013. Belgium: CoESS – Confederation of European Security Services, 255 p. Retrieved from http://www.coess.org/newsroom.php?page=facts-and-figures

[343] Ibid

minimum criterion for the age, but it ranges from 18 to 21 years. In Lithuania, Latvia, Croatia, Finland, France, Austria, Greece, Luxembourg, the Netherlands and other EU countries, the required minimum age of all private security employees is 18. However, in some EU countries (Belgium, Poland, Estonia, Denmark, Romania, Slovenia), this requirement is differentiated into two age groups:

1) individuals over the age of 18 years, where private security staff are assigned to a basic level of security activities that does not need a license, i.e. operational staff;
2) individuals from the age of 21 years old, where private security officers are assigned as managers or must have a higher qualification to work in high risky business sector (banks, airports, seaports, bodyguarding, in-cash transit operations) or state-owned strategic objects (nuclear power plants, oil factories, electricity grid companies, some paramilitary objects).

The research carried out by the author reveals that in many EU countries there are no separate requirements for private security managers and security guards who are directly engaged in the implementation of the security functions. There is a contradiction in legal regulation in determining the requirements for age criteria, when the same age limit applied both to the manager of a private security company and to a security guard or employee. Naturally, a reasonable question arises as to whether a person under the age of 18 years old can professionally manage a private security company. Only a few EU countries set the minimum age for private security managers: 21 years old – Belgium, Romania and Slovakia, 22 years old Sweden and 25 years old – Denmark. Hence, it is necessary to clearly distinguish a criterion of age requirement applied for managers of the private security companies and other security employees. It could be argued that a person under the age of 25 years may have entrance and be recruited as a manager of a private security company, and persons aged 18 or over – as security guards. The main argument setting a 25-year old age requirement to the manager of the private security company is that a person's managing activities of private security company must comply not only with the general requirements, but, additionally, with the specific requirements (for instance, have a higher education, working experience and so on). Private security business is not just a simple business; it is carried out with high commitment and responsibilities and is constantly balancing to the emergence of legal consequences. Therefore, the manager of the private security company must have organizational, planning, coordination, information analysis, critical thinking, analytical and prognostication skills. Similarly to police services, which must meet high requirements for providing public security services to society.

The author proposes to legislatively delimit the age requirement and to consolidate various professional competence requirements for the private security staff engaged in providing unarmed security services (18 years), the private security staff engaged in providing armed security services (from 21 year) and for private security company manager (25 years).

1.2. Educational requirements for the private security employees

The national legislation of the Member States requires that persons admitted to work in private security company at least must have secondary education. Only in the Netherlands, Malta and Serbia national law set a requirement to have a vocational education before entrance to private security company. It shows that individuals must complete the appropriate vocational (basic) training before starting work at the private security company. Despite the fact that CoESS and UNI-Europa in collaboration with social partners developed *The European Vocational Training Manual for Basic Guarding (1999)*[344], in which was outlined the minimum basis for the training of security guards throughout Europe at national level. However, nowadays there is no common EU provision on appropriate level of education, which a person who wants to work in the private security sector should have.

Today, each Member State sets the minimum requirements for basic training of the private security guards at its discretion. Concerning education requirement and basic training the differences varies from EU countries were vocational training is obligatory for any employee entering the private security sector to countries where there are no regulations at all. In EU countries, the duration of vocational training for private security workers varies greatly, i.e. from a few hours to a year, from officially developed and approved training programs to several training courses (2 or 3), from basic training provided voluntarily in-house by a private security company to specialized training institutions.

According to the data analysis presented in CoESS report[345], the minimum education requirement for private security employees

[344] The European vocational training manual for basic guarding (December 1999). Belgium: CoESS – Confederation of European Security Services, UNI-Europa: European services workers union, 164 p. Retrieved from https://www.eesc.europa.eu/resources/docs/138-private-act.pdf

[345] Private Security Services in Europe: CoESS Facts and Figures 2013. Belgium: CoESS – Confederation of European Security Services, 255 p. Retrieved from http://www.coess.org/newsroom.php?page=facts-and-figures

is 120 hours to follow basic guard training. For instance, Austria and Poland are an example of a state with particularly weak regulations on training for private security employees; indeed, the duration of basic training is 8 hours and training is organised on the company level and upon successfully completing the basic training, private security guards are not issued with a certificate of competence. A similar situation is in Cyprus, the Check Republic, Italy, where there is no obligation for private security guards to follow basic guard training, but in Cyprus the chief of police may ask candidates for a licence to undergo specialised training, in order to be able to obtain a licence (depending on their previous experience).

The most demanding country in educational area is the Netherlands where there is an obligation for private security guards to finish 1 year of basic guard training and get a diploma before starting to work in the private security industry, as well as Romania, where 360 hours of basic guard training is required, Hungary – 320 hours, Sweden – 288 hours, Spain – 180 hours, Latvia – 160 hours, France – 140 hours and Belgium – 127 hours. Moreover, the minimum number of hours of basic guard training varies greatly with some countries such as Greece (105 hours), Slovenia (102 hours), Croatia, Denmark, Finland, Ireland (100 hours), Germany and Luxembourg (80 hours), whilst UK requires only 20 hours, Malta – 30 hours, France – 32 hours, Bulgaria, Germany, Slovakia – 40 hours, Estonia – 50 hours, Lithuania – 52 hours and Portugal – 58 hours. It should be noted that in above-mentioned EU countries upon successfully accomplishing the basic training, private security guards are issued with a certificate of competence.

Some Member States have fixed in national laws a mandatory requirement to finish specialised training for private security managers, i.e. operational managerial staff influencing operations (from site supervisor to CEO). This educational requirement is applied in Finland, Hungary, Ireland, Portugal, Slovakia, Spain and other EU countries. For instance, in Belgium middle management or private security companies should have finished 52 hours and higher supervisors 100 hours of specialised training; in Estonia, Slovenia and Germany – 80 hours of mandatory specialised training exists for private security managers, in Sweden – 44 hours, in Romania – 120 hours, in Poland – 245 hours and in Greece – 360 hours.

There are also differences in the number of training sessions that private security employees must take as a follow-up every year. Refresher training is compulsory in some Member States and varies widely in terms of both the volume of hours required and frequency. For example, Spain and Portugal requires employees to undergo 20 hours' refresher training per year, while Sweden requires one week every three years, Bulgaria and Belgium requires 32 hours every five years.

It can be seen, in the Member States exist different regulations of educational requirements for private security employees. The main reason for this is the diversity of EU countries national policies on the private security employees training. Fact should be taken into consideration that requirement for persons to have a minimum level of education (secondary or basic in short-term) differs from higher education in terms of both the specific knowledge gained and the acquired professional skills and values. Vocational training does not really extend the professional competence of private security employee and does not give sufficient knowledge of why certain rules or procedures must be followed in one way or another when providing security services. It would be appropriate to consider the possibility of unifying educational requirements for the private security employees combining elements of vocational training with higher education.

1.3. Other specific requirements for private security employees

A comprehensive overview of the private security sector landscape in EU Member States allows to identify variety of some other requirements which are fixed in EU countries national laws. According to CoESS report[346], these requirements could be divided into two groups: *entrance requirements* and *specific requirements* for security employees. Generally, the following *entrance requirements* for private security employees are applying in EU countries:

1) nationality. In all Member States, candidates must be a national of the country or of another EU state. Only France does not have any nationality criteria;
2) health. In many EU countries, applicants to private security company must be in good health and provide a medical certificate from a public hospital (both physical and mental health), which is renewed from every two (Slovakia, the Czech Republic, Hungary, Slovenia) to five years (Cyprus, Greece, Lithuania, Estonia, Finland, Spain). For example, in Sweden the requirement to be in good health regulated only if the security guard is working at night;
3) physical fitness. Some EU countries required from candidates of private security company the proof of good

[346] Private Security Services in Europe: CoESS Facts and Figures 2013. Belgium: CoESS – Confederation of European Security Services, p. 255. Retrieved from http://www.coess.org/newsroom.php?page=facts-and-figures

physical aptitude (Croatia, Luxembourg, Portugal, and Slovakia);

4) language. Member States legalisation has a provision that the requirement to have proficiency in the national language may apply for private security employees. Latvia, Estonia, Slovenia, Sweden and the Netherlands require from candidates to speak fluently in the official language and it is mandatory to work in the security industry. Spain requires that candidates to private security company must speak Spanish or a regional language if employed in the Basque or Catalan reģions;
5) military or public security service. Greece requires its security employees and security managers to have completed their military service. In Spain and Malta, candidates to private security company must not have been discharged from the armed or security forces, in Portugal – from information services or public security forces;
6) double-jobbing. Legislation in some EU countries prohibited for candidates to private security company to work in the private investigation sector (Belgium, Spain and the Netherlands), national or foreign defence (Slovenia), or in arms sales (Belgium and Portugal). For instance, Belgium required not being a member of the police force during the last 5 years;
7) incompatibility with a previous occupation. The public authorities in some Member States require that individuals have not previously worked in the public security sector in recent years (two years for Spain and five years for Belgium, France and Portugal);

8) residence. In all Member States, for candidates to private security company is enough to have a primary residence in one of the Member States of the EU. Croatia, Slovakia and Estonia additionally require to have a permanent address or residence permit and registered residence in the country. For non-Cypriots, a period of six months' residence in Cyprus is a prerequisite. Romania and Estonia requires candidates to have a national citizenship or status of permanent resident.

All EU countries have *specific requirements* related with the following issues:

1) mandatory to provide security services in the uniforms. Private security employees' uniforms must be easily distinguishable from those of the police force, fire and rescue service, customs officials or prison guards. Bodyguards are not required to wear a uniform. Only in Belgium, uniforms are not compulsory, but if they are being used, they must be clearly distinguishable from those worn by the police, military and other public security officers;
2) mandatory to have identification cards of private security personnel. The ID card must bear a photo and the employee's personal security code and company name;
3) clean criminal record, no court convictions, penal and pre-trial proceedings. For example, Malta has regulated that applicants must not be convicted of crimes against persons or property fined over € 2,329 or crimes against public trust and not have been convicted in the last five years;

4) background screening and/or a testimonial of good moral character;
5) application fee. Some EU countries have a rule, that candidates pay fixed fee for submission of application with all supporting documentation and after that – annual fee (Denmark, Malta, Cyprus).

M. Button and P. Stiernstedt[347] agreed, that professional requirements for candidates to private security companies additionally can be extended to such requirements as minimum share capital (requiring a minimum share capital for owners), authorisation of other Member States' training/professional qualifications, setting minimum for the number of employees in undertaking, issuing multiple licences for the security company within Member States.

Analysis of professional requirements for private security employees showed that in the EU exist regulatory diversity setting entrance and other specific requirements and it would be a reasonable decision to standardize it in the future. Proposed relevant and problematic assertions imply that Member States must start the discussion on the establishment of uniform standards of professional requirements for private security personnel.

2. Recognition and unification of private security employees' professional competences

Professionalism and the quality of security services provided by private security staff leads to professional knowledge and skills, abilities and values. V. Cortese, H. de Clerck and other authors argue,

[347] Button, M., Stiernstedt, P. (2017). The evolution of security industry regulation in the European Union. *International journal of comparative and applied criminal justice*, Vol. 41 (4), pp. 245–257

that the scope of private security employees' professional competences is determined by learning content and learning outcomes.[348] It was noted, that in the EU area, there still has not been developed a security guard training standard, which would legitimize the private security employees' fields of activities, professional competences and their limitation, learning objectives and assessment methods of professional competences.

Research studies identified the normative regulatory gaps in the field of private security guard education and training among Member States and existing discrepancies to the common principles of EU law.[349] This causes problems trying to describe what kind of professional knowledge and skills are necessary for private security personnel, which evaluation criteria is necessary to establish and how to evaluate their professional competences. Due to the legal uncertainty of private security employees' professional competence

[348] Cortese, V., Dryon, P., Martinez, E. (2008). The modernization of work organization in the European private security industry: final report of the European project VS/2007/0235. Bruxelles: the Centre of Sociology of Work, the Université Libre de Bruxelles, p. 32;

Clerck, de H., Lindstrom, M. (2009). Private and public security in the Nordic countries. Belgium: CoESS General Secretariat, Sweden: Almega private security, p. 23

[349] Born, H., Caparini, M., Cole, E. (2007). Regulating private security in Europe: status and prospects. Geneva: Geneva Centre for the Democratic Control of Armed Forces: *Policy Paper,* No. 20. Retrieved: from: https://www.dcaf.ch/sites/default/files/publications/documents/PP20_Born_Caparini_Cole_.pdf;

Kalesnykas, R., Dieninis L. (2012). Professional competences (training standards) of private security guards: the need for identification and legal regulation. *Current Issues of Business and Law*, Vol. 7, No. 1, pp. 164–182;

Button, M., Stiernstedt, P. (2018). Comparing private security regulation in the European Union. *Policing and society: an international journal of research and policy*, Vol. 28 (4), pp. 398–414 in the normative documents, private security companies apparently lost the advantage over other security services providers in the security market, i.e. police, border guard service, public security forces, private detectives or fire and rescue officers. According to this, it is useful to find the right definition, scope and content of private security guards' professional competence, also highlight an importance of professional competence in security guards operations and the requirements for establishing legal and regulatory issues.

2.1. Definition of private security employees' professional competence

Profession – *security guard* – in the EU is considered as a new type of labour profession. The employment of private security guards seem to be similar to other professions such as police officers, but they receive different legal status in the society and different support as related to the similar challenges they encounter with other employees from the security sector. In some EU countries (UK, Denmark, Sweden, the Netherlands) security guard profession was not recognized within the private security industry until three decades ago and today is considered one of the constantly changing social professions in labour market. Cambridge dictionary defined that *security guard* is a person employed to protect a building against intruders or damage; someone whose job involves preventing people going into places without permission, transporting large amounts of money, or protecting goods from being stolen.[350] *A security guard* (also known as a security officer or security agent) is a person employed by a public or private security

[350] Cambridge dictionary (2018). Retrieved from https://dictionary.cambridge.org/dictionary/english/security-guard

sector to protect the employing security sector's assets (property, people, equipment, money, public order, etc.) from a variety of hazards (such as waste, damaged property, unsafe worker behaviour, criminal activity such as theft, etc.) by enforcing preventative measures.[351] Security guards do this by maintaining a high-visibility presence to deter illegal and inappropriate actions, i.e. looking directly (through patrols) or indirectly (by monitoring alarm systems or video surveillance cameras) for signs of crime, taking actions to minimize damage and reporting any incidents to their clients and emergency services (such as the police or paramedics).

Term *security guard profession* is inseparable from the term of the profession in the general sense, according to which the profession is defined as any type of work that needs special training or a particular skill, often one that is respected because it involves a high level of education.[352] The profession is occupation, practice, or vocation requiring mastery of a complex set of knowledge and skills through formal education and/or practical experience.[353] Every organized profession (security guard, police officer, attorney at law, etc.) is governed by its respective professional body. Consequently, the *security guard profession* is a permanent security service activity based on relevant knowledge, practical skills and abilities.

Any person's ability to perform a specific job is called professional competence. Professional competence means a functional ability to carry out certain activities in an adequate manner, have

[351] Santonen, T., Paasonen, J. (2017). Evaluating the adequacy of private security industry regulation in Finland. *Security Journal*, Vol. 30, Issue 2, pp. 585–604

[352] Cambridge dictionary (2018). Retrieved from https://dictionary.cambridge.org/dictionary/english/security-guard

[353] Business dictionary (2018). Retrieved from http://www.businessdictionary.com/definition/profession.html

enough knowledge and skills to ensure a high-quality and competent job assignment in a real practical situation. Private security guards profession consists of a multitude of related elements of professional competences: functions and tasks, rights and obligations, forms and methods of activity, for which certain preparation is required. The importance of private security employees' professional competence is greater wherewith more significant their role in the security market.

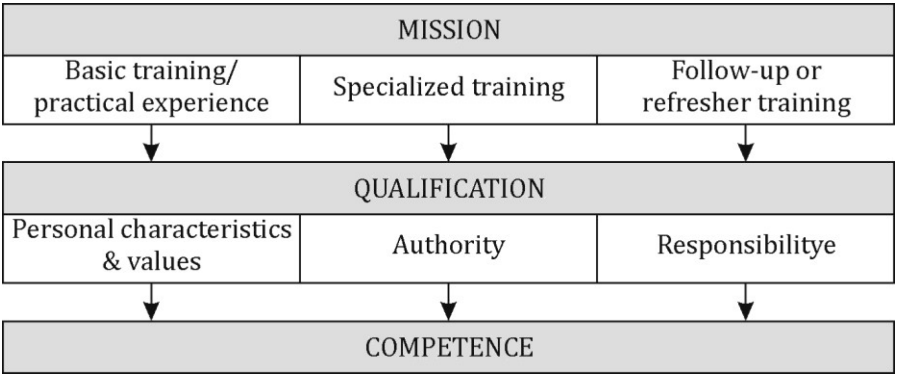

MISSION
Basic training/ practical experience
Specialized training
Follow-up or refresher training
QUALIFICATION
Personal characteristics & values
Authority
Responsibilitye
COMPETENCE

Figure 1. **Concept of private security employees' professional competence**

Figure 1 shows, that private security employees' professional competence depends from acquired knowledge, practiced skill and capacity building, which can be used in providing high-quality security activities. Professional qualification is a fixed category, expressed in a certain document (diploma) attesting of the acquired education in accordance with the relevant professional (or vocational) training and the study program.

Nowadays, there are four types of security guard professions identified within the private security industry, which include: the contract security profession, the in-house security profession, private central alarm monitoring station and high security profession.[354] The name given to the different types of private security profession derives from the functions expected to be performed by the security guards under the profession. According to J. J. de Waard, contract security guards are individuals performing activities on professional basis for a third party and their objective is the preservation of the security of person and property or maintenance of public law and order[355]. It shows that competence, not qualification enables a person to act in different, ever-changing conditions of activity.[356] Consequently, private security employees' professional competence reflects such professional skills and abilities, knowledge and experience that enables them to act and react in different situations of practical work.

2.2. Scope and content of private security employees' professional competences

In a constantly evolving social environment, the development of professional competencies for private security employees is becoming a major guarantee for the provision of service quality in the private security market. Due to the rather wide range of security services and their scope, only basic knowledge and practical training in providing various security services are not enough for the private

[354] De Ward, J. J. (1999). The private security industry in international perspective. *European journal of criminal policy and research*, Vol. 7 (1), pp. 143–174

[355] Ibid

[356] Kalesnykas, R. (2007). Privatization processes of policing in Lithuania. *SIAK Journal: Zeitschrift für Polizeiwissenschaft und Polizeiliche Praxis*. Wien: Bundesministerium für Inneres, No. 3, pp. 14–24

security employees. Although in some EU countries (Belgium, Croatia, Austria, Finland, France, Greece, Hungary, Lithuania, Slovenia), private security employees are trained in security training institutes (centres) according to adequate curricula, but the content and scope of these study programs are different and determined by national regulatory rules on vocational training. As was mentioned above, one of the security industry regulatory weaknesses is the lack of common security employees' training (and education) standard in the EU area. According to it, a specialized study program could be approved and upon completion of which the appropriate level of education (third and/or sixth, seventh level) is acquired and the professional qualification is given – the security guard or security officer.

Current and future generations of security guards will have to be more competent on various levels of skills and attitudes. Different and evolving educational needs and requirements emerge. Training on legal requirements, knowledge of rules and regulations will remain elementary and might even have to be intensified in an environment where criminality is still a strong concern for citizens and organizations and where the private security industry will get an ever increasing importance in assisting and complementing public law enforcement agencies in fulfilling a societal duty of crime prevention and protection in risky situations.[357]

It is assumed that the quality of security services and professional activity of private security employee is determined by: (a) knowledge and skills; (b) adequate physical condition; (c) foreign

[357] The new security company: integration of services and technology responding to changes in customer demand, demography and technology (5th White Paper, Berlin, 23 April 2015). Belgium: CoESS – Confederation of European Security Services, 52 p. Retrieved from http://www.coess.org/newsroom.php?page=white-papers

language skills; (d) computer literacy; (e) the pursuit of professional development; (f) essential characteristics of the employee concerned. S. Dadelo, who has explored the determinants of the security guards professional competencies, concludes that the activities of a security guard are also determined by macro-factors such as theoretical and practical readiness, professional activity, mental characteristics, biological development, motor, physical and tactical skills.[358] In the private security employee's professional training should be developed the following ordinary (basic) skills:

1) loyalty to the security guard profession;
2) ability to act in stressful situations (to take the right decision);
3) ability to listen, communicate and solve practical problems;
4) physical and combat readiness;
5) desire to work in the team;
6) language proficiency;
7) use information and working with IT;
8) continuous development and improvement of new professional knowledge.

Taking into account specific knowledge, skills or abilities, for private security employees should be described the following competences (training institutions should focus on these in education):

1) *personal competences,* through which these individual characteristics of the security guard are developed: responsibility, honesty, reliability, integrity, self-confidence, initiative, punctuality, tidiness, commitment, endurance;

[358] Dadelo, S. (2011). *The effectiveness of physical education, its diagnostics as an educational factor*. Vilnius: Technika, p. 74

2) *subject-matter competences,* through which are developed security employee's respect for human rights and freedoms, respect for the rule of law, the perception and compliance of business moral norms and social values, and the ability to reconcile conflicting social interests;
3) *social (legal liability) competences,* through which security employee's behaviour, communication with clients and law offenders, ability to adapt in a dynamically changing environment, take decisions that are consistent to changes, provision of security services according to defined standards, ability to form a positive image of the private security company are developed.

CoESS experts[359] distinguish three levels of private security employees' professional competence:

1) performing tasks in accordance with vocational education and training (VET) standards. This level of professional competence can be achieved through introductory (or basic) training programs designed to provide basic guidelines (principles) of mastering and acquiring operational methods to all private security employees. Also, develop the general skills to implement task effectively, make right decisions, carry out assignments dedicated to the

[359] Cortese, V., Dryon, P., Martinez, E. (2008). The modernization of work organization in the European private security industry: final report of the European project VS/2007/0235. Bruxelles: the Centre of Sociology of Work, the Université Libre de Bruxelles, p. 25;

Private security and its role in European security (5th White Paper, Paris, December 2008). Belgium: CoESS – Confederation of European Security Services, 98 p. Retrieved from http://www.coess.org/newsroom.php?page=white-papers competence of private security companies, and professionally provide security services to clients and other customers. In all EU countries, there is an obligation for private security guards to follow basic training. Basic training programme is mandatory by law and upon successfully accomplishing basic training, private security guards are issued with a certificate of competence;[360]

2) improvement of professional qualification through regular development of practical skills. To achieve this level of professional competence, follow-up or refresher training programs for security employees' qualification improvement are used. The aim of these training programs – provide necessary knowledge and skills for private security staff in order for better performing their duties and functions, or to achieve higher positions in the private security company;
3) interdisciplinary or integrated training. This level of professional competence requires knowledge that is covered by interdisciplinary studies and is needed to solve various complex issues related with risk or crisis situations.

Today, customers expect much more from private security staff, such as conflict handling skills or language skills in a growing international and multi-cultural environment. This is more of an attraction point for younger generations as in many EU countries they are growing up in multicultural and multilingual contexts.

[360] Private Security Services in Europe: CoESS Facts and Figures 2013. Belgium: CoESS – Confederation of European Security Services, p. 255. Retrieved from http://www.coess.org/newsroom.php?page=facts-and-figures

Conversely, such professional requirements are not as obvious for many older security guards who want to stay on. Guarding was accessible in the past for people with lower qualifications and the private security industry has done many efforts to change this, by recruiting more qualified employees and/or by investing in in-house training.[361] For instance, in alarm receiving centres and video surveillance rooms, the technical and IT-level of the operators must follow the specifications of the technological solutions installed and connected. However, on customers' premises or in mobile operations, security guards will have to become and remain familiar with the use of electronic security platforms they have to operate in a local control centre, or with tablets or other devices used in the professionalized process approach of guarding activities.

Currently, private security employees' education, training and/or lifelong learning are implemented at different levels. The objective of such training at different levels is to realise a minimum standard for every security guard in a private security company. It could provide and guarantee the necessary knowledge and skills needed for performance of security services. Private security employees' training at different levels is focussing on easy to measure performance emphasising observation techniques, written and oral reporting, social skills and customer approach, efficient and effective operation. Table 1 presented a detailed overview of training content of the way leading to professional qualifications at different security levels. Some training topics that may be included additionally: the role of security guards and their legal powers and limitations, access control,

[361] The new security company: integration of services and technology responding to changes in customer demand, demography and technology (5th White Paper, Berlin, 23 April 2015). Belgium: CoESS – Confederation of European Security Services, 52 p. Retrieved from file: http://www.coess.org/newsroom.php?page=white-papers

safety and hazardous materials, communications and report writing, public and client relations and customer service, professional ethics and conduct and other topics specific to certain private security sector.

Table 2

Content of private security employees' professional

Education and training levels				
Guarding	**Mobile services**	**Technical services**	**Management skills**	**Large-scale security**
Basic Commercial manned In-house manned Event Door supervision (bouncing) Bodyguarding Canine services Ascertaining material facts Stewarding Fire prevention and protecting services Safety of track construction Receptionist/concierge services Firearms	Beat patrol Mobile alarm response and call-out services Cash-in-transit services Transporting goods and valuables	Alarm control Alarm installation CCTV monitoring	Security risk management Loss prevention Private investigation Security consulting Store detective Emergency and disaster management	Aviation security Maritime security Urban security (train/metro stations, city patrols) Cybersecurity Critical infrastructure protection Guarding military units

The ambition to unify private security guards basic training was presented in CoESS report named "European Vocational Training Manual for Basic Guarding" (1999).[362] Such training manual describes

[362] The European vocational training manual for basic guarding (December 1999). Belgium: CoESS – Confederation of European Security Services, UNI-Europa: European services workers union, p. 164. Retrieved from https://www.eesc.europa.eu/resources/docs/138-private-act.pdf

scope and content of the skills that should be gained and reflects the minimum level security employees should master. The units of the European Vocational Training manual for basic guarding are the following: (1) private security industry; (2) security guard: status and competence; (3) security equipment; (4) practical security procedures; (5) emergency procedures; (6) law and the basic guard; (7) health and safety; (8) first aid; (9) customer care & quality of services; (10) communications; (11) labour relations and labour regulations. Of course, some of the training units have to be modified to meet the specific national context of Member States, for instance, when it concerns national legislation or other characteristics of the national peculiarities as to wherein private security is embedded. This is something to be judged upon by the social partners on a national level, whenever necessary in close co-operation with respective national authorities and training providers.

It's important to keep in mind, that a record of the training, reflecting when a private security employee received training, what that training consisted of, and the form of testing and its results, should appear in the employee's personnel file. In the event of a subsequent critical incident, this documentation enables the private security company to demonstrate how employees were trained to follow policies and procedures. Helping to raise minimum standards, this practice could also help to limit the private security company's liability for any misconduct by a security employee.

Summing up the importance of security employees' professional competence in the private security market, it can be seen that the determination of the security employees' professional competences and their boundaries resolves two interrelated problems: *firstly,* in the Member States exiting a separate vocational training system for security guards should meet the EU's uniform requirements for professional and competent private security market as well as customers and society needs; *secondly,* it justifies the need to develop the security training standard and according to its established education system (vocational and higher) and study programs, upon completion of which the person would be awarded with security qualification and a higher education diploma. In order to ensure that a competent employee independently performs security guard services in accordance with the security training standard, it is necessary to precisely identify the scope and content of their professional competences, describe appropriate training objectives and select clear assessment methods of professional competences. This could be a starting point for further discussion on the development of a uniform security training system across the EU.

3. From the diversity of training levels to a common private security training standard

Despite the diversity of professional requirements and training levels that exists in Member State private security sector, it is required to form the starting point towards the development of universal professional standards for private security employees. Standardisation of pre-assignment training, certification requirements, and in-service training, is necessary. Private security industry minimum standards in terms of selection, recruitment, education and training and supervision of security personnel should be identified and enforced in order to increase the professionalism of the security sector generally. This ambitious task is faced by global challenges (including socio – political and legal factors) to private security industry.

Indeed, in the EU countries there is no standardisation on the level of training required in order to become a private security employee. There is a huge difference in the performance of the security services and in a way, private security sector is imbedded in legislation throughout the Member States. As was stated before in this article, private security employees' education and training varies from EU countries were vocational training is obligatory for any employee entering the private security sector to EU countries where there are no regulations at all. Whilst some EU countries require the training to be regulated by the Ministry of Interior (Belgium, Croatia, Finland, Estonia, Latvia, Lithuania, Spain) others suggest that voluntary in-house company training is sufficient (Italy, Cyprus, the Czech Republic, Poland).

Strengthening security-related training infrastructure in the area of security related education and training; the EU security market appears to be highly fragmented.[363] Current training initiatives for security functions and tasks are highly diversified, with a very large number of small public and private operational training centres (often) under direct control of local authorities or a specific public service. For example, in most of the EU countries (Romania, Finland, Cyprus, Spain, Lithuania, Estonia, Latvia, etc.) the public authorities play a key role in the provision of security staff training. First of all, police officers determine training content and course curriculum, which is then submitted to police managers for approval. Further, facilitators must be approved by the Ministry of Internal Affairs or the head of national police department. Finally, exam committees must include at least one police officer. In France

[363] The socio-economic added value of private security services in Europe (2013). Belgium: CoESS -Confederation of European Security Services, p. 27. Retrieved from file:///D:/Downloads/wp-4-2013-the-socio-economic-added-value-of-private-security-services-in-europe.pdf

and Belgium, private security in-house training centres must be approved by the Department of Home Affairs. Sweden has certified security training institute set up by the private sector and approved by the Ministry of the Interior. In Germany, training content is determined at the federal level and provided by the Chambers of Commerce and by professional associations in the sector. The German Federal Government finances the training of job seekers to facilitate their access to the private security market. In Slovakia, training is provided by private organisations. However, teachers are required to show evidence of at least five years' work experience in this area and must obtain a licence issued by the Ministry of the Interior, which is valid for 10 years.[364]

To exemplify, the case of an appropriate level of mandatory training addresses not only the proficiency and efficacy of security personnel, but would also negate many of the identified weaknesses of the industry. Such weaknesses can be the abuse of authority, excessive use of force, low professional standards, and non-compliance with the law. M. Button and P. Stiernstedt[365] in their research shows (Table 3), what is the current situation of private security training in some EU countries. It is an evidence that some Member States have a clear regulatory issues on providing professional education and training (Belgium, Spain, Slovenia, Sweden, Greece, Portugal); the rest fall below this, with a handful mandating

[364] Private security and its role in European security (Fifth White Paper, Paris, December 2008). Belgium: CoESS – Confederation of European Security Services, p. 98. Retrieved from http://www.coess.org/newsroom.php?page=white-papers

[365] Button, M., Stiernstedt, P. (2018). Comparing private security regulation in the European Union. *Policing and society: an international journal of research and policy*, Vol. 28 (4), pp. 398–414

no or little more than a few days entrance or basic training (Austria, Cyprus, Czech Republic, Ireland, Malta, Italy, France, UK).

Table 3

Comparison of training levels for private security employees in EU countries

Member State	Licensing of training	Mandatory training	Exam	Refresher training	Specialized training	Management Training
Austria	+	2	–	–	–	–
Belgium	+	14	+	+	+	+
Bulgaria	+	6	+	–	+	+
Croatia	+	12	+	–	+	–
Cyprus	+	–	–	–	–	–
Denmark	+	12	+	–	–	–
Estonia	+	8	+	–	–	+
Finland	+	12	+	–	–	–
France	–	8	+	–	–	–
Germany	+	+	+	–	+	+
Greece	+	14	+	+	–	+
Hungary	+	14	+	–	+	–
Ireland	+	4	–	–	+	–
Italy	+	–	+	–	+	–
Latvia	+	14	+	–	–	–
Lithuania	+	6	+	–	–	–
Luxembourg	+	10	+	+	+	–
Netherlands	+	14	+	–	–	–
Poland	–	14	–	+	–	+
Portugal	+	6	+	+	+	+
Romania	+	14	+	–	+	–
Slovenia	+	10	+	+	+	+
Slovakia	+	6	+	–	–	+
Spain	+	14	+	+	+	+
Sweden	+	14	+	+	+	+
Malta	+	4	+	+	+	–

<table>
<tr><th>Member State</th><th>Licensing of training</th><th>Mandatory training</th><th>Exam</th><th>Refresher training</th><th>Specialized training</th><th>Management Training</th></tr>
<tr><td>UK</td><td>–</td><td>6</td><td>+</td><td>–</td><td>+</td><td>–</td></tr>
<tr><td>Czech Republic</td><td>–</td><td>–</td><td>–</td><td>–</td><td>–</td><td>–</td></tr>
<tr><td colspan="7">Licensing of training. To provide training of security, staff is required a license: if yes (+), and if not (–).
Mandatory training stipulated by the legal regulation. The range of hours, whose maximum value is justified, provide the following range of points: 0 hours = 0, 1 to 19 hours = 2, 20 to 39 hours = 4, 40 to 59 hours = 6, 60 to 79 hours = 8, 80 to 99 hours = 10, 100 to 120 hours = 12 and 121 + hours = 14.
Exam. Upon successfully completing the basic training is there a theoretical and/or practical pass/fail exam after which private security guards are issued with a certificate of competence (+), and if not (–).
Refresher training. If exist mandatory refresher or follow-up training (+), if not (–).
Specialized training. If mandatory specialist training is required for security roles other than general guarding then (+) and if not (–).
Management training. If mandatory training is required for management roles of private security company, then (+) if not (–).</td></tr>
</table>

** Source: M. Button and P. Stiernstedt*[366]

Provided examples verify the assumption that it is necessary to establish a unified private security training system within the Member States. Before it would be expedient:

1) assess the current situation and the role of the private and public sector training infrastructure in the security field. This would allow to provide a basis for a comprehensive support framework for the development and enhancement of security training facilities and infrastructure;

[366] Button, M., Stiernstedt, P. (2018). Comparing private security regulation in the European Union. *Policing and society: an international journal of research and policy*, Vol. 28 (4), pp. 398–414

2) develop an EU initiative aimed at strengthening the provision of security related education and training. This could incorporate the creation of a network of security training institutions at the EU level. Such a network would provide a platform for internal exchange of best practice, cross-border training initiatives, etc. with the aim of overcoming the difficulties posed by the fragmentation in the private security training domain.[367]

By agreeing with R. Sarre and T. Prenzler[368] position, in this case more palatable would be a new EU directive that sets out the basic minimum requirements for security education and training in all Member States. A new EU directive could set basic requirements for the licensing of individuals and training institutions and draw out some of the minimum standards they should meet. Such EU level regulation should touch not only traditional private security field of activity, but also specific business service sectors, such as commercial bank security, cybersecurity, airport security, maritime security, protection form piracy and so on.

Nevertheless, even this in the current security politics of the EU, with some Member States such as the UK (and others) pursuing less European-level intervention, combined with the strains on some common security apparatus such as the borderless arrangements of

[367] Study on the competitiveness of the EU security industry (15 November 2009). The Netherlands, Rotterdam: ECORYS. Retrieved from https://ec.europa.eu/growth/content/study-competitiveness-eu-security-industry-0_en

[368] Sarre, R., Prenzler, T. (2011*). Private security and public interest: exploring private security trends and directions for reform in the new era of plural policing*. Sydney: Australian Security Industry Association, p. 58

the Schengen area would be unlikely.[369] Despite this, developing a private and public sector training infrastructure and establishing European-level security training system should be the priority for the policymakers and social partners of the European private security industry. There should be greater investment of the Member States in the development of a common security training model around the building blocks of an effective regulatory system. European-level private security training standard could include the three key elements: first, regulatory system and rules; second, education and training for all of the common roles; third, licensing requirements for training institutions and individuals.

To sum up, it could be stated that one of the main goals of the standardization of the security training is to develop a European wide education and training structure that will affect both the level of professionalism and the image of the private security sector. The idea to develop private security training standard with Member States should be widely debated nationally and is to be set as a minimum regulatory guidelines and training programmes in the EU according to national and international law. There is no doubt that the developed private security training standard and professional qualifications of security employees will be useful for security managers as a guide to skill levels in company and in private security service in general. Professionalization is achieved through the establishment of standardized requirements for private security employees' education and training which could significantly increase quality of security, trust and image of private security companies

[369] Button, M., Stiernstedt, P. (2017). The evolution of security industry regulation in the European Union. *International journal of comparative and applied criminal justice*, Vol. 41 (4), pp. 245–257

throughout the EU and its society. The professional standardization of security guards training and development will do the private security industry a justice in forever changing business landscape and clients' needs.

Conclusions and recommendations

1. Summing up research results, it could be suggested that setting professional requirements for private security employees in regulatory framework should solve two problems: *first,* substantiate the need of developing education and training programs for private security personnel leading to professional qualification and higher diploma and, *secondly,* private security education and training system should comply with that of the Member States to meet the requirements for professionalism and competiveness of private security staff as well as clients' and customers' needs.
2. The author concluded that the regulatory framework (EU directive) and clear setting of professional requirements for private security staff predetermine the legitimacy of the implementation of powers and obligations of private security guards, the professionalism of providing security services and the success of private security business. Professional requirements for private security personnel should reflect not only their special training but also the compatibility of education and provided security duties.
3. It is evident that in the Member States the private security sector is prevailed by different models of security staff training, i.e. higher education and vocational training that does not create a common private security training system to ensure competence, expertise and professional requirements of private security

personnel. Private security employees training could be more efficient as a result of combining higher education (theoretical and analytical knowledge) and vocational training (practical skills) models.

4. Private security services employees should meet contemporary educational standards through a developed unified European-level security training program. Training providers should be able to use such standard for ensuring the quality of education. Private security training standard and professional qualifications will be useful for employers as a guide to knowledge and skills levels in private security sector. The standard also could provide a benchmark for the design and delivery of various training by employers (for instance, mandatory basic training, refresher training, specialised training for specific industry segments). Individuals will have proof of professional competence and will enhance the opportunities to gain employment and to possibly move within and outside their present area of work (employability).

References

Berg, J. (2007). *The accountability of South Africa's private security industry: mechanisms of control and challenges to effective oversight*. Newlands, South Africa: Criminal Justice Initiative of the Open Society Foundation for South Africa, p. 39

Born, H., Caparini, M., Cole, E. (2007). Regulating private security in Europe: status and prospects. Geneva: Geneva Centre for the Democratic Control of Armed Forces: Policy Paper No. 20. Retrieved from https://www.dcaf.ch/sites/default/files/publications/documents/PP20_Born_Caparini_Cole_.pdf

Business dictionary (2018). Retrieved from http://www.businessdictionary.com/definition/profession.html

Button, M. (2007). Assessing the regulation of private security across Europe. *European Journal of Criminology*, Vol. 4(1), pp. 109–128

Button, M. (2008). *Doing security: critical reflections and an agenda for change*. Houndmills, UK: Palgrave Macmillan, p. 264

Button, M., Stiernstedt, P. (2017). The evolution of security industry regulation in the European Union. *International journal of comparative and applied criminal justice*, Vol. 41 (4), pp. 245–257

Button, M., Stiernstedt, P. (2018). Comparing private security regulation in the European Union. *Policing and society: an international journal of research and policy*, Vol. 28 (4), pp. 398–414

Cambridge dictionary (2018). Retrieved from https://dictionary.cambridge.org/dictionary/english/security-guard

Clerck, de H., Lindstrom, M. (2009). *Private and public security in the Nordic countries*. Belgium: CoESS General Secretariat, Sweden: Almega private security, p. 43

Collins, S. C., Britto, S., Britto, M. (2008). High-school private security programs: the wave of the future? *Security Journal*, No. 21, pp. 159–172

Cortese, V., Dryon, P., Martinez, E. (2008). *The modernization of work organization in the European private security industry: final report of the European project VS/2007/0235*. Bruxelles: the Centre of Sociology of Work, the Université Libre de Bruxelles, p. 50

Dadelo, S. (2011). *The effectiveness of physical education, its diagnostics as an educational factor*. Vilnius: Technika

De Ward, J. J. (1999). The private security industry in international perspective. *European journal of criminal policy and research*, Vol. 7 (1), pp. 143–174

Kalesnykas, R. (2002). Possibilities to integrate the private security in the system of law and order. *Jurisprudence: academic journal of Mykolas Romeris University*, No. 26 (18), pp. 71–82

Kalesnykas, R. (2005). The threat as a dimension for security industry development. *Jurisprudence: academic journal of Mykolas Romeris University*, No. 76(68), pp. 102–112

Kalesnykas, R. (2007). Privatization processes of policing in Lithuania. *SIAK Journal: Zeitschrift für Polizeiwissenschaft und Polizeiliche Praxis*. Wien: Bundesministerium für Inneres, No. 3, pp. 14–24

Kalesnykas, R., Dieninis, L. (2010). The legal regulation of professional requirements for private security personnel: the experience of Lithuania and some European Union countries. *Current Issues of Business and Law*, Vol. 5, No. 1, pp. 223–241

Kalesnykas, R., Dieninis, L. (2012). Professional competences (training standards) of private security guards: the need for identification and legal regulation. *Current Issues of Business and Law*, Vol. 7, No. 1, pp. 164–182

Montgomery, R., Taylor, C. (2015). *The use of private security services for policing*. Ontario, Canada: Public Safety Canada

Private security and its role in European security (Fifth White Paper, Paris, December 2008). Belgium: CoESS – Confederation of European Security Services, p. 98. Retrieved from http://www.coess.org/newsroom.php?page=white-papers

Private Security Services in Europe: CoESS Facts and Figures 2013. Belgium: CoESS – Confederation of European Security Services. Retrieved from http://www.coess.org/newsroom.php?page=facts-and-figures

Santonen, T., Paasonen, J. (2017). Evaluating the adequacy of private security industry regulation in Finland. *Security Journal*, Vol. 30, Issue 2, pp. 585–604

Sarre, R., Prenzler, T. (2011). *Private security and public interest: exploring private security trends and directions for reform in the new era of plural policing*. Sydney: Australian Security Industry Association

Study on the competitiveness of the EU security industry (15 November 2009). The Netherlands, Rotterdam: ECORYS. Retrieved from https://ec.europa.eu/growth/content/study-competitiveness-eu-security-industry-0_en

The European vocational training manual for basic guarding (December 1999). Belgium: CoESS – Confederation of European Security Services, UNI-Europa: European services workers union, p. 164. Retrieved from https://www.eesc.europa.eu/resources/docs/138-private-act.pdf

The new security company: integration of services and technology responding to changes in customer demand, demography and technology (Fifth White Paper, Berlin, 23 April 2015). Belgium: CoESS – Confederation of European Security Services, 52 p. Retrieved from http://www.coess.org/newsroom.php?page=white-papers

The socio-economic added value of private security services in Europe (2013). Belgium: CoESS – Confederation of European Security Services, 27 p. Retrieved from file:///D:/Downloads/wp-4-2013-the-socio-economic-added-value-of-private-security-services-in-europe.pdf

About the Author

Raimundas Kalesnykas, *Prof. Dr.*
Raimundas Kalesnykas is a lecturer at the Faculty of Law of the Kazimieras Simonavicius University in Vilnius, Lithuania. He graduated in law and security studies within security manager specialization (BA, Master and PhD) at the Law University of Lithuania. Raimundas Kalesnykas has more than 20 years of professional experience as a researcher, academic, trainer (ToT), published more than 50 books and research papers, presented research results in over 80 international scientific conferences in Lithuania and abroad, as an invited professor, visited over 60 foreign universities for lecturing, successfully

implemented over 30 international projects on issues of security and anti-corruption risk management and strategical solutions, police, criminal justice and security sector reform. He has over 14 years' professional experience working as a key security and anti-corruption expert in OSCE, USAID, Saferworld and other

GUIDELINES FOR SECURITY STAFF TRAINING AND EVALUATION COMMUNICATION

Stanislav Dadelo

1. Security staff evaluation and training communication problems

The range and quality of services offered depend not only on the market demand but also on the quality and competence of the security staff. The human factor is essential in the area of security. In the super-competitive world, it is usually the competent staff of company – or company's "human resources" – not its machinery that determines the company's competitive edge. Three-fourths of the total losses sustained by a company appear due to inadequate actions taken by its staff; 80 percent of non-disclosure of secrets is caused by correct selection, employment and preparation of staff.[370] In big enterprises, staff management issues are settled by personnel units. When working with personnel, the following goals are vital:

1) determination of specific professional qualities of workers (education, age, gender, biological data, mental qualities, intellectual level);
2) search for and recruitment of prospect workers (employment advertisements in papers and internet; addressing employ-ment agencies, etc.);

[370] Dadelo, S. (2011). The effectiveness of physical education, its diagnostics as an educational factor. *Review. Social sciences, educology* (07S). Vilnius: Technika

3) selection of candidates (testing, interviewing, conversations, appraisal);
4) preparation of newly-employed workers;
5) management, control and evaluation of workers' professional performance.

Thus, one of the most important tasks assigned to a personnel unit is to select and employ only such persons who inspire confidence and who are very promising because losses brought about by bad workers exceed losses produced by external threats.

In the area of security, services of the highest quality will be provided by those enterprises, which have a good strategic plan for staff management – personnel recruiting, selection, training and remunerating. In order to elicit higher labour efficiency from security staff, it is necessary to create a penalty and bonus system. When discussing staff members' remuneration within the context of the personnel strategic management plan, it is necessary to pay more attention to the appraisal and training communication of personnel. Appraising personnel is a complex task; it covers the evaluation of such issues as personnel's ability to work, personality, behaviour, compatibility, potential, and talents. This in its turn includes the evaluation of separate personality qualities which a very numerous. Therefore, discussing the staff management plan outlined by a business providing security services it is vital to characterise and evaluate a security worker (guard, officer) profession, and requirements for personal qualities.

When appraising staff management at private businesses providing security services, personnel criteria (motivation, law, powers, professional preparation, experience, etc.) come into focus. Security business belongs to the area of services, so the qualities of staff determine not only the commercial success of a security services-providing business but also the commercial success, health, and life of the client to whom a particular security service is sold. In case of a guarded object, 80 percent security is determined by organisational measures, 16 percent by mechanical and architectural means, and 4 percent by electronic and information equipment.[371] The efficiency of organizational security measures directly depends on the qualification and discipline (loyalty) of staff. It is necessary to characterise special qualities of a security worker profession, and requirements for security staff personality.

2. Professional duties performed by a security staff

In the modern world, human activity may be called profession on the condition that it conforms to a number of formal criteria:

1) formal training for a particular profession is provided;
2) special training programmes for this profession have been created;
3) there is a formal procedure providing for the acquisition of an official document proving that relevant professional qualification has been acquired;
4) there is a list of personal qualities necessary to this profession, and a system for their evaluation (personal qualities may include practical skills, intellect, psychological portrait, theoretical knowledge, physical abilities, health condition, etc.).

The basis of profession acquisition is a pedagogical process. The principal goal of the pedagogical process is goal-oriented education

[371] Nowicki Z. T. (1999). *Ochrona osób i mienia*. Toruń

of a human. Humans achieve their best professional performance results at 40–50. There is a highly-developed professional education system in the world; it is used by people of different age. Oxford Dictionary defines profession as a paid occupation, especially one that involves prolonged training and a formal qualification.

Security worker profession, as defined by its current notion, emerged not long ago. Positions and professions connected with security are quite numerous; they can be found in police and state border guard forces, or army, or civil safety, special service, health cares, fire prevention, labour protection system; security workers act in the capacity of specialists, guards and watchers; their purpose is to protect people. Security workers are also regarded as workers securing protection to society.

ESCO European Classification of Skills/Competences, Qualifications and Occupations assigns security staff to Personal service, administrative support service, security, and investigation activities. The International Standard Classification of Occupations[372] (ISCO) places the security worker profession in the "Service sphere". Professions included in this group require knowledge and abilities to provide services to individuals and to sell goods in the market. Basic tasks are connected with travel, household, personal care and property protection, order and law maintenance, and sale of goods and services. Most of these professions require a second ISCO-88 qualification level. Having in mind that ISCO-88 classifier provides four qualification levels, security workers have to meet very high requirements for qualification.

[372] ESCO: European Classification of Skills/Competences Qualifications and Occupations, (2013). Retrieved form: http://bookshop.europa.eu/en/esco-european-classification-of-skills-competences-qualifications-and-occupations-pbKE0313496

Security staff must be divided by specific character of tasks performed by security workers: watchman guarding an object, watchman-administrator of an object, armed security guard protecting an object, rapid response unit member, cash collection and values' transportation security guard, bodyguard. National legislation must consolidate the practice of appraising qualifications possessed by security workers; licensing to carry out safety works of different character must provide for appraisal of security workers' competences.

3. Requirements for security staff personal characteristics

Requirements for security worker's personal characteristics.

Oxford Dictionary defines protection as the action of protecting or the state of being protected. The process of guarding is understood as prevention of all types of losses appearing due to some causes. In general, it is possible to state that guarding means all measures connected with the prevention of losses appearing due to human or natural influence; it also means maintenance of order and prevention of offence or other erroneous and damage-inducing actions. It is necessary to characterise general targets set for a security worker. So, the security worker's targets include:

1) the protection offered to a person – actions aiming to secure the safety of the protected person's life, health and inviolability;
2) property protection – actions barring the way to the emergence of offence and attacks against private property as well as actions barring the way to the offence which is committed at the moment against private property, and to persons having no right to visit guarded territories.

Insufficiently qualified security workers pose a criminal attack risk in the security business. When generalising statistics of criminal attacks against guarded objects, it is necessary to note that reliable correlation was found between the preparedness of security staff and the probability of attack. It must be stated that legislation usually does not provide any relationship between the level of private security staff's qualification and the probability of risk posed to the guarded object and/or person, or their dangerousness. So, employers must take up personnel selection and appraisal practice themselves.

A security worker in the line of duty can resort to restraint by physical force and special measures. A multitude of methodological aids for training private security workers have been developed.[373]

Aids intended for the training of security staff describe activities and situations in a methodological way. However, it remains not clear what particular qualities should distinguish a security worker; this is important in order to achieve maximally efficient performance.

Experience accumulated by security businesses has formed the principles of appraisal and differentiation of guarded objects. Key criteria for the appraisal of objects are related to the character of risk and the probability of its emergence. Appraisal of a guarded object enables to identify essential qualities and working tasks of security staff. The tasks may include cybernetic, technological, criminal, natural or other threats. Dangerous situations do not emerge daily; probabilities of their emergence differ in separate

[373] Hilyer, B., Veasey, A., Oldfield, K., Craft-McCormick, L. (1999). *Effective Safety and Health Training*. Boca Raton: CRC Press;

Rudofossi, D. (2012). *A Street Survival Guide for Public Safety Officers*. New York: Routledge;

Button, M. (2007). *Security Officers and Policing*. London: Routledge;

Brislin, R. F. (2014). *The effective security officer's training manu*al. Oxford, UK: Elsevier, Butterworth-Heinemann objects. Specific qualities of security worker's professional performance are determined by his environment (Figure 1). In order to ensure that the security worker will carry out his duties efficiently, it is essential to appraise the security worker's environment, his personal qualities, and his history.

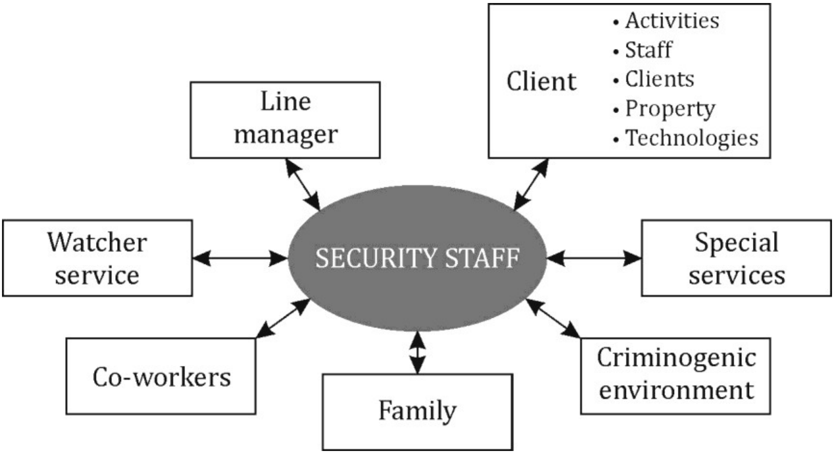


Figure 1. **Environment in which a security staff performs his duties**[374]

Appraisal of the security worker's environment makes the levels of requirements for his particular qualities obvious. In major businesses providing safety services with all guarded objects are divided into groups by various criteria; security workers are appraised and awarded corresponding qualification categories, giving them a chance to work either in more or less important objects.

General working assignments in any security worker's professional activity are universal:

[374] Dadeło S. (2005). Czynniki determinujące kompetencje pracowników ochrony na Litwie. Wydawnictwo AWF Warszawa. Warszawa–Vilnius

1) foreseeing dangers, threats, and risks of various backgrounds;
2) avoiding or eliminating the causes (dangers, threats, and risks) due to which danger may emerge;
3) reacting adequately and efficiently to an unexpected dangerous event;
4) eliminating negative consequences of the dangerous event;
5) adapting one's manner and looks to the image created by client and/or security firm (employer).

Performance of professional duties by a security worker is connected with emergencies and threats of various backgrounds. This creates pre-requisites for characterising the specific qualities to be possessed by a security worker:

1) to be able to evaluate a situation instantly;
2) to be able to gather and analyse information;
3) to determine the sort and character of danger;
4) to be able to make correct decisions swiftly;
5) to have confidence-inspiring looks;
6) to show initiative;
7) to be able to solve conflict situations;
8) to be reliable at work;
9) to be able to react to criticism correctly;
10) to be polite and know etiquette rules;
11) to be guided by firm moral principles in society and family;
12) to obey instructions and laws;
13) to be psychologically harmonised with colleagues and clients;
14) to be ready to risk;
15) to be able to do monotonous work and be resistant to fatigue;
16) to be ready for a physical close fight, including an armed clash.

Security worker's professional performance is connected with the risk of physical force. What personal characteristics are required by a situation of physical encounter? Involved in a physical combat situation, the security worker must demonstrate specific psychophysical characteristics and special combat training. A person involved in combat actions should be characterised by independent thinking; creativeness; concentration; control of emotions. In the event of an attack reaction to the attacker's action is usually delayed, there is not time to evaluate the situation and use available measures safely and in conformity with the law.

4. Factors, determined professional competences of security staff

A person who has just started his professional career must satisfy two conditions: the person must be able to work, and he must wish to work. Personal ability to work is described by the following formal requirements: a spotless reputation and an adequate health condition. Personal desire to work is described by motivation. There are very many motives encouraging an individual to engage in professional activities; the character of these motives differs (material, spiritual, emotional, etc.). When describing professional performance results, dominant motives should be specified.

One of the principal forms of human activity is professional work. Here a question arises: which factors decide that a human takes up and pursues some profession? Selection of a particular professional direction is determined by genetic, social and psychological factors; they have different meanings.[375] As for the choice of a security worker profession, it should be made clear what served as an incentive to make such a choice and which factors were decisive.

Security worker profession demands specific knowledge, skills and abilities as well as biological, physical and mental qualities. Knowledge possessed by a security worker determines his ability to work; his motivation determines his willingness to work; and his health condition, psychological characteristics, biological indicators, general and special physical preparedness indicators, special abilities and skills determine his fitness for work. If one of these conditions weakens, it is impossible to expect from a security worker any reliable performance. Here we have another question: which factors are decisive in professional activities and how they affect each other? All factors determining the efficiency of professional performance are divided into external (social environment: state, organizations, family, etc.) and internal (individual characteristics: inborn and acquired) ones.

Six groups of factors determining the efficiency of professional performance of security staff are distinguished (Figure 2). Grouping human activity-determining factors is a relative path. When doing it, it is necessary to take into account the weight of factors, and the influence made by these factors on the final efficiency of performance.

[375] Dadelo, S., Turskis, Z., Zavadskas, E. K., Dadeliene R. (2015). Integrated multi-criteria decision making model based on wisdom-of-crowds principle for selection of the group of elite security guards. *Archives of budo*, No. 9(2). pp. 135–147

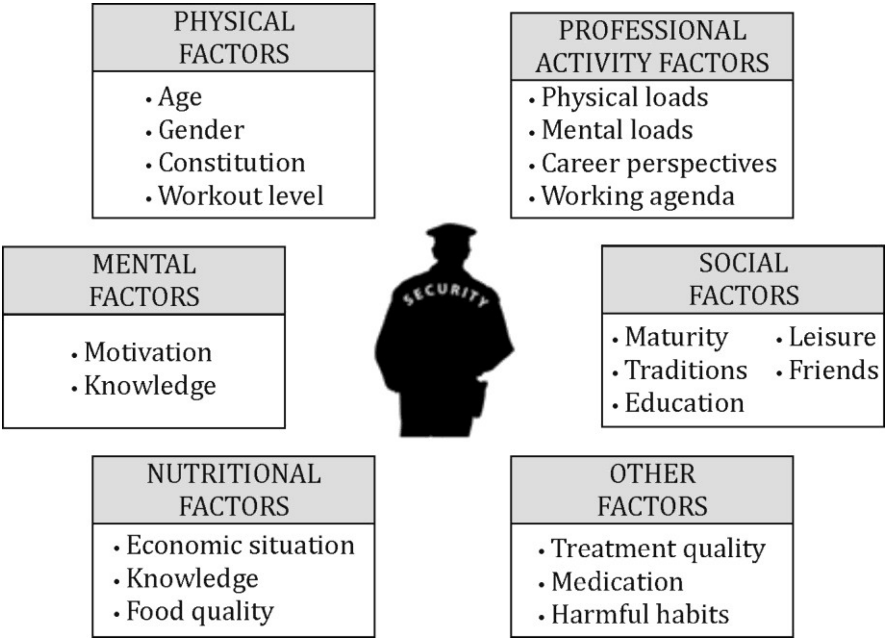


Figure 2. **Factors determining the efficiency of human professional performance**[376]

Forming security staff it is essential to clarify which factors influence the effectiveness of work. There are three main conditions for a person to effectively act in the professional field, namely, capability, knowledge and willingness. Consterdine[377] in the description of security staff selection principles distinguished the main factors that should be taken into account. They are physical qualities, psychomotor function, and psyche and personality values.

[376] Rikspolisstyrelsen (1987). *Fisisk Traning*. Stocholm

[377] Consterdine, P. (2007). *The Modern Bodyguard: The Complete Manual of Close Protection Trainin*g (Self defense). Somerset

Our research has revealed the relevance of macro factors in the staff selection process: theoretical and practical preparedness, professional activeness, psychic peculiarities, biological development, motor and fighting skills.

According to experts, all these qualities are essential in successful professional practice. Essential differences have been pointed out in evaluation among leadership and security staff. More mature age and longer working experience are considered more important by the leaders; whereas the staff emphasise physical preparedness, social trends and capabilities of operating weaponry and tactical efficiency. Research into private, civil sector and control group security staff has lead to grouping professional competence determining factors into macrofactors; a system of those factors was formed, and inside and outside estimation was given (Figure 3).

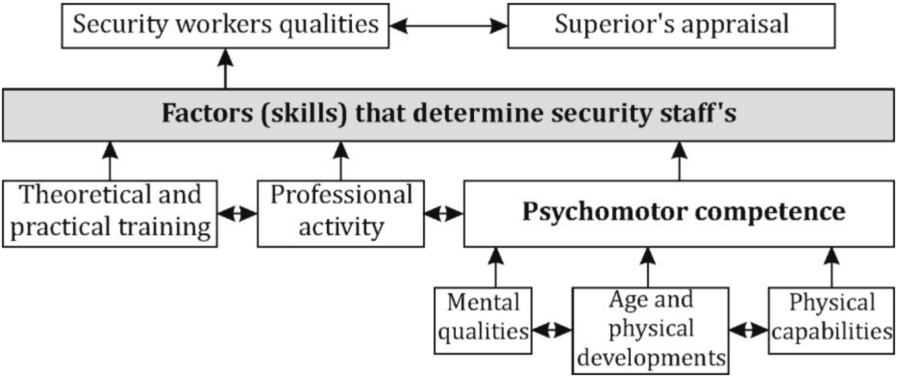

Security workers qualities
Superior's appraisal
Factors (skills) that determine security staff's
Theoretical and practical training
Professional activity
Psychomotor competence
Mental qualities
Age and physical developments
Physical capabilities

Figure 3. **Factors (skills) that determine security staff's competencies**[378]

[378] Dadelo, S. (2011). The effectiveness of physical education, its diagnostics as an educational factor. *Review. Social sciences, educology* (07S). Vilnius: Technika

Correlation between psychobiological and social features was researched; they were identified by grouping test indices; all data were normalized and quantitative indices of the factors were calculated (Table 1).

Table 1

Correlation of the analysed indices of security staff (n = 118)

Indices	Theoretical and practical preparedness	Profes-sional activity	Age and physical develop-ment	Motor skills	Fighting skills	Mental features	Direct superior‘s appraisal
No	1	2	3	4	5	6	7
1	1.00						
2	0.06	1.00					
3	**0.22**	**0.29**	1.00				
4	0.06	0.03	–0.07	1.00			
5	**0.21**	**0.27**	**0.24**	**0.30**	1.00		
6	**0.22**	0.00	**0.22**	0.11	**0.21**	1.00	
7	**0.31**	**0.57**	**0.39**	–0.06	**0.30**	0.10	1.00

p<0,05 (r=0,195); p<0,01 (r=0,254); p<0,001 (r=0,321)

Fighting skill capability factor has a reliable correlation with all other factors researched. Therefore, the factor demonstrating security staff's acting capability in an encounter is one of the key elements indicating qualification, preparedness; it is vital in choosing a task and selecting the staff. The importance of fighting skills (correlation with motor capabilities) has led to the question: which of the physical qualities have the strongest effect on the success of fighting actions and how they are related to the factor of biological development? Separate physical quality indices were normalized and grouped into distinct macrofactors. From the analysis of correlation of fighting, motor capabilities and biological development, we can see that the fighting skills of security staff only have a correlation with physical agility and biological development. Physical development can be essential to fighting capability if opponents are of different biological development. It must be noted that physical development has a reliable negative correlation with the quality of endurance.

Having analysed the summarized factors affecting security staff's professional competence, having estimated their factor weight and comparative analysis with superiors' appraisal of particular factors, a significant difference appeared between inner and outside evaluation indices.

Research into the indices determining professional competences of security staff has revealed that there are three main physical qualities producing the strongest impact, namely, agility, endurance, strength. Research has shown that fighting capacity effectiveness quotient (the number of fights won from the total number) reveals the security staff's fighting skills best of all.

Research into security company superiors' appraisal and comparison with the data found through security staff's analysis, has revealed which of the factors have the strongest influence on security staff's competence; the method of factor analysis calculating the present correlations were used. It was discovered that the competence of security staff is basically determined by mental qualities (22 %), age and physical development (20 %), physical preparedness (16 %), professional activity (15 %), theoretical and practical preparedness (14 %) and fighting capabilities (13 %).

The fighting skills of security staff are determined by all summarized factors, however, there is very little or no correspondence to the particular test or measurement indices.

Similar results were received in a similar research where the same methods were used in combination with a similar form of testing. Nevertheless, summarization into a single index of physical qualities has led to a strong correlation with fighting skill factor. Fighting skill test results are highly informative as their summary leads to indirect information concerning other factors that influence security staff's professional competence.

5. Guidance for security staff evaluation and training

Professional activities of security guards encompass observation, help and conflict resolution. The possibility of threats faced may depend on the value of the guarded objects. Actions can be classified into the following stages: threat and offence identification, analysis of the situation, prediction of possible consequences and solution methods, choice of a solution and the solution itself.

Resolved situations, including conflicts, may differ in intensity, level of danger and dynamics; all this depends on the influence of a security guard. In conflict situations with offenders, the security guard must be capable of influencing the opponent psychically, using physical force, special means and weapons. The security guard must be aware of his/her personal responsibility when making decisions especially in cases where physical contact cannot be avoided and fighting efficiency is necessary. Fighting efficiency, depending on the intensity of resistance and the level of danger, can be classified as follows:

1) minor offence – verbal communication (giving information on responsibility, consequences and requirements);

2) passive resistance (ignoring requirements) – handling the situation (giving orders, non-verbal warning acts, arrest);
3) active resistance (avoiding physical contact, active resistance) – restriction technique application (act of strangling or attempts to cause pain);
4) active attack with an aim to cause physical damage (strikes, attempts to cause pain when striking or strangling) – self-defence techniques and adequate use of special means (strikes, attempts to cause pain when striking or strangling);
5) active attack actions aimed at serious physical damage – self-defence techniques, the use of special means and adequate use of a weapon.

Professional competences with the factors that determine them and their correlation enable selection; psychomotor competence that determines defence skills, morphologic, psychological qualities and their theoretical and practical preparedness are regarded as important factors. The factor of physical preparedness is also one of the elements.

Evaluation criteria aimed at estimating guards capabilities provide us with the level of their abilities and enable to optimise professional training. Having assessed the factors that determine competences, the possible findings lead to the presumption that distinctive features are typical of those belonging to the superior group.

Factor analysis applied for the assessment of security staff's competence has shown that in the internal appraisal (of summarised identified variables) all professional competence factors reliably correlate with fighting skills; no other factor assessed reveals such efficiency; therefore, when researching fighting skills such methods should form the qualification criteria basis. It is essential to focus on the improvement of fighting skill in the system of security staff training and education.

Security staff could be classified according to tasks they are responsible for: security staff of an object, administrative security staff of an object, armed security of an object, rapid response crew, armed security guard, cash and valuables transportation security guard and staff security guard. It is essential that employers focus on staff selection and take action to evaluate and rate and prepared candidates. This process requires defining key competencies of a security guard and rating them depending on aims and possible threats at work.

References

Anderson, G. S., Plecas, D., Segger, T. (2001). Police officer physical ability testing. Policing: *An International Journal of Police Strategies & Management*, No. 24(1), pp. 8–31

Arvey, R. D., Landon, T. E., Nutting, S. M., Maxwell, S. E. (1992). Development of Physical Ability Tests for Police Officers: A Construct Validation Approach. *Journal of Applied Psychology*, No. 77(6), pp. 996–1009

Brislin, R. F. (2014). *The effective security officer's training manual*. Oxford, UK: Elsevier, Butterworth-Heinemann

Button, M. (2007). *Security Officers and Policing*. London: Routledge

Consterdine, P. (2007). *The Modern Bodyguard: The Complete Manual of Close Protection Training* (Self defense). Somerset

Dadelo, S. (2011). The effectiveness of physical education, its diagnostics as an educational factor. *Review. Social sciences, educology* (07S). Vilnius: Technika

Dadeło, S. (2005). *Czynniki determinujące kompetencje pracowników ochrony na Litwie.* Wydawnictwo AWF Warszawa. Warszawa–Vilnius

Dadelo, S., Turskis, Z., Zavadskas, E. K., Dadeliene, R. (2015). Integrated multi-criteria decision making model based on wisdom-of-crowds principle for selection of the group of elite security guards. *Archives of budo*, No. 9(2), pp. 135–147

ESCO: European Classification of Skills/Competences Qualifications and Occupations, (2013), Retrieved from http://bookshop.europa.eu/en/esco-european-classification-of-skills-competences-qualifications-and-occupations-pbKE0313496

Hilyer, B., Veasey, A., Oldfield, K., Craft-McCormick, L. (1999). *Effective Safety and Health Training*. Boca Raton: CRC Press

International Labour Office (ed.) (1990). *ISCO-88. International Standard Classification of Occupations*. Geneva: ILO

Nowicki, Z. T. (1999). *Ochrona osób i mienia*. Toruń

Rikspolisstyrelsen (1987). *Fisisk Traning*. Stocholm

Rudofossi, D. (2012). *A Street Survival Guide for Public Safety Officers*. New York: Routledge

About the Author

Stanislav Dadelo, *Prof. Dr.ph.* Vilnius Gediminas Technical University
S. Dadelo brings more than 25 years of professional work experience in various internal affairs of Lithuania and private security areas including security staff training. Author of the scientific monograph “Factors Determining of Competences Lithuanian Security Workers”. Creators of bachelor's study program “Security systems engineering” in Vilnius Gediminas Technical University. Member in editorial boards of six scientific journals. Science and practice internships in Sweden, French, Denmark, Malta, Portugal, Germany, Poland, Check Republic, People's Republic of China etc.

Part V

Physical security

STRUCTURAL SECURITY

Ryšardas Burda

The structure of the safety of the enterprise depends on many indicators of the enterprise, on the context of the enterprise. Depending on the context of the enterprise risks of the enterprise differ. Any security system first of all, shall react to risks of the enterprise.

Risk – the situation connected with existence of the choice from estimated alternatives by assessment of probability of approach of the event attracting both positive and negative effects.

The efficiency of the organization of risk management in many respects is defined by the opportunity for effective application of the corresponding methods and acceptances of risk management. Risks of the enterprise: internal and external, their classification can be according to the characteristics.

Natural – belong the risks of natural disasters, such as earthquakes, floods, hurricanes, typhoons, lightning strokes, eruptions of volcanoes, etc.

Technological hazards are connected with business activities of the person. The mixed risks are the events of natural character which became result of business activities of the person.

Static – are connected only with losses in business activity. It is a risk of losses of real assets owing to causing damage of property.

Speculative or dynamic risks are risks of unexpected changes of cost estimates of management decisions of firm and also changes of the market relations or political circumstances.

Industrial hazards are the risks characteristic of productive activity and productions connected with losses from the stop for the different reasons and also with inadequate use of the equipment and technology, the fixed and revolving funds, production resources and working hours.

Financial risks are the risks connected with probability of losses of financial resources (money). Financial risks are subdivided into two types: the risks connected with purchasing power of money and the risks connected with capital investments (investment risks, credit risks, risks of real financial loss). As losses financial risks divide into the direct property risks and risks connected with obligations i.e. risk of losses because of competitors, employees or partners in connection with changes of conditions of accomplishment of obligations.

Property risks are the risks connected with the possibility of losses of property for the different reasons: thefts, diversions, negligence, overvoltage of technical and technological systems, damage, etc.

Commercial are connected by risks with the business activity oriented to receiving the maximum profit and arising in implementation process of the goods and services made or purchased by the enterprise.

Social risks are directly connected with life, health and working ability of employees of the enterprise and also their personal characteristics and working conditions.

Entrepreneurial risk is connected with accidental losses of the entrepreneurial profit. Losses in business activity divide on material, labor, financial, dead times and special types of losses.

The organization of the security police of the enterprise shall correspond to certain principles. There are different classifications of the principles of creation of the security system of the enterprise:

1) legality;
2) complex use of forces and means;

3) coordination and interaction in and out of the enterprise;
4) competence;
5) economic feasibility;
6) planned basis of activity;
7) system;
8) the priority died warnings (timeliness);
9) continuity;
10) economy;
11) interaction;
12) combination of publicity and confidentiality;
13) complexity;
14) echeloning;
15) reliability;
16) reasonable sufficiency;
17) continuity.

Safety of the enterprise shall be:

1) continuous;
2) planned;
3) centralized;
4) active;
5) reliable;
6) universal;
7) complex.

However, not only trailers of creation of system of the enterprise matter for the organization of security service of the enterprise and also creation of structure of safety. Legal regulation of activity of security companies and legal opportunities of activity of security companies and their package of the provided services have a great influence.

Types of service which security services are allowed to provide to the enterprise (or functions of the security service):

1) identification of unfair competition from other enterprises;
2) collecting data on criminal cases;
3) investigation of the facts of disclosure of a trade secret of the enterprise;
4) collection of information about the persons which concluded the contract with the enterprise;
5) search of the lost property of the enterprise;
6) investigation of the facts of unauthorized use of commodity (company) signs of the enterprise;
7) search of missing employees;
8) identification of insolvent partners;
9) identification of unreliable business partners;
10) collecting data on civil cases;
11) studying of criminal and negative aspects of the market;
12) collection of information for carrying out business negotiations;
13) protection of life and health of personnel against illegal encroachments;
14) protection of property of the enterprise;
15) providing an order in venues the enterprise of representative, confidential and official actions;
16) consultation and providing recommendations to the management and personnel of the enterprise for questions of safety;
17) design, installation and operational service of means of the security and fire alarm system.

A security worker, while exercising personal and property safety, is entitled to:

1) to carry and use a firearm;
2) to carry and use special measures, as well as to use physical violence;
3) suspecting that a person is preparing to commit or commit an administrative violation of law or a criminal act, request the cessation of unlawful acts;[379]
4) to arrest the suspected violator of law, encountered in the course of an administrative violation of law or a criminal offense related to the protected object or entity, or immediately thereafter. The detained person must be immediately transferred to the police;
5) to inspect the identity documents of a protected object and to establish an identity, to inspect the items held by persons, as well as to inspect the goods in the means of transport and documents related thereto, if the permit regime exists in that facility;
6) having the data to suspect that in the protected object an administrative violation of law or a criminal act is being prepared, is being committed or has been committed, to require the suspected offender to reveal the possessions with them and to examine them with his or her oral or written consent. If there is a written consent of the suspected offender, you can also view the person himself. In addition to the required consent, the employee is not entitled to inspect the items specified in this item and the person;

[379] Personal And Property Safety Law of the Republic of Lithuania; 2004 m. liepos 8 d. Nr. IX-2327, Vilnius, 1041010ISTA0IX-2327

7) by a written instruction of the management body of a client, legal entity, another organization or its unit containing a security unit to exclude persons other than officials and other persons who are entitled to this right by the law in a protected object.[380]

Unlike an employee of a security guard who carries out personal and property security, the activities of a private detective are regulated by another legal act. The activities and the rights of a person and property security employee and a private detective are different. Therefore, the organization often needs to adapt to the situation and deal with the felony due to the qualifications of the security staff and their licensing.[381]

1. Missing or according to the law recognized untraceable persons search, the disappearance of fact finding, information about the possible location of their collection.
2. The parents (adoptive parents), guardians or caretakers request information about minor children (adopted children), performing in a particular field and limited factors in a specific area of persons

[380] Personal And Property Safety Law of the Republic of Lithuania; 2004 m. liepos 8 d. Nr. IX-2327, Vilnius, 1041010ISTA0IX-2327

[381] Law of the Republic of Lithuania on Private Detective Activity; TAR, 30-04-2005, No. 6577;

Law on Criminal Intelligence of the Republic of Lithuania; State News, 20.10.2012, No. 122-6093;

The Code of Criminal Procedure of the Republic of Lithuania; State Gazette, 09-04-2004, No. 37-1341;

Law on the Legal Protection of Personal Data of the Republic of Lithuania; State News, 03-07-1996, No. 63-1479;

Law on State and Service of Secrets of the Republic of Lithuania; State Gazette, 9-12999, No. 105-3019;

Other (total 89 acts)

according to the law under guardianship or trusteeship, the behavior and the surrounding environment collection and research.

3. Collection and investigation of information necessary for criminal proceedings.
4. Collection and investigation of information necessary for the investigation of civil disputes.
5. Collection and investigation of information necessary for the investigation of labor disputes.
6. Collection and investigation of information required for the investigation of disputes arising out of insurance contracts.
7. Collection and investigation of information necessary for the processing of administrative justice cases.
8. Collection and research of the client's origin, kinship, biography and other customer data.
9. Customer's commercial, industrial and (or) trade secrets protection, technical security holder (legal manager) premises, vehicles or other legally managed client sites, as well as electronic information storage and electronic communications devices, protection against unauthorized gathering technical information measures.
10. The client stolen, missing, or otherwise wasted forfeited assets or the ownership of the property document, or other information relating to property search.
11. Preparation of confidentiality meetings.
12. Consultation on other issues of private detective activity.
13. Assessment of the credibility and solvency of individuals.
14. Collection of data on unfair competition or commercial activities.
15. Finding Debtors and Their Property.

The quantitative and qualitative analysis of threats allows to draw a conclusion that reliable protection of the economy of any company is possible only at integrated and system approach to its organization. Among the main objectives of a security system of the enterprise of any commercial structure are:

1) protection of legitimate rights and interests of the enterprise and its employees;
2) collecting, analysis, assessment of data and forecasting of development of a situation;
3) studying of partners, clients, competitors, candidates for work for companies;
4) timely identification of possible aspirations to the enterprise and its employees from sources of external threats to security;
5) prevention of penetration of the enterprise from the structures of economic intelligence of competitors, organized crime and individuals with illegal intentions;
6) counteraction to technical penetration in criminal intents;
7) identification, prevention and suppression of possible illegal and other negative activity of staff of the enterprise to the detriment of its safety;
8) protection of staff of the enterprise against violent encroachments;
9) ensuring safety of the material values and data which are a trade secret of the enterprise;
10) getting of necessary information for development of the most optimal administrative solutions on strategy and tactics of economic activity of the company;
11) physical and technical protection of buildings, constructions, territory and vehicles;
12) formation among the population and business partners of the favorable opinion on the enterprise promoting implementation of plans of economic activity and the authorized purposes;

13) compensation of the material and moral damage caused as a result of illegal actions of the organizations and individuals;
14) control of efficiency of functioning of a security system, improvement of its elements.

Treat basic elements of a security system of the enterprise:
1) protection of a trade secret and confidential information;
2) IT safety;
3) internal security;
4) safety of buildings and constructions;
5) physical safety;
6) technical safety;
7) safety of communication;
8) safety of economic and contractual activity;
9) safety of transportation of goods and persons;
10) safety of advertising, cultural, mass activities, business meetings and negotiations;
11) fire safety;
12) ecological safety;
13) radiochemical safety;
14) competitive investigation;
15) information and analytical work;
16) propaganda providing social and psychological, precautionary scheduled maintenance among personnel and its training in question of economic security;
17) expert check of the mechanism of a security system.

The economic security of an enterprise (organization) is the state of the most effective use of corporate resources to prevent threats and create conditions for the stable functioning of its main divisions.[382]

In this section we will examine specific elements of the security structure and their content. Structure of Security service can consist of:

1) group of the mode. Defines the list of the data which are a trade secret, exercises control of order of classification of documents and etc.;
2) technical group. Together with group of protection participates in safety of activity of an object (by means of technical means of protection – the systems of the alarm system, observation, communication, etc.);
3) detective group. Develops and holds special events for studying of individuals from among personnel of an object, clients of firm and inhabitants of the environment next to an object, whose actions contain threats to security of activity of an object (firm);
4) protection posts. Post – it charged to the security guard (I guard) the site of work (the building or its site, the room, the territory, etc.) on which it has to provide during the certain time (provided by the sheet on point duty or the sheet of a post) the protection mode according to the received instructions;
5) means of communication. Now effective activity of any kind of institutions and enterprises is impossible without application of a radio communication. The fast, convenient and reliable communication is necessary first of all between

[382] Kormishkina, L.A. (2011). *Methodical instructions on the organization of the self-governing work of course hearings economic safety of the enterprise* (organization). Saransk

posts of protection of an object and also between all employees of group on duty of protection for rapid response to any kinds of violations of the mode of protection, the organization of counteraction to threats and fast evacuation of people at emergence of dangerous circumstances;

6) means of protection. Now for protection of objects technical means of protection are very widely used – it is the various equipment, devices, devices and designs intended for detection and definition of threats, creation of barriers on the way of their distribution;
7) special means of protection. Special means of protection are intended for safety of a commercial object from different types of unauthorized information retrieval and also protection against radiation exposure;
8) system of protection of objects. At the heart of the development of the system of protection of an object and the organization of its functioning, lies the principle of creation of consecutive boundaries and safety zones in which threats have to be in due time found, and their distribution will be interfered by reliable barriers. Such boundaries have to settle down consistently, from a fence around the territory of an object to the main thing, especially important room, such as storage of values and commercial information.

Conclusions

1. The security structure and organization of the security has taken on the corporate context.
2. The context of an enterprise is important in identifying certain risks that can be external and internal.

3. A risk-management company must follow the chosen principles and create a non-essential safety system, depending on the needs of the company, large business, etc.
4. Different countries have different regulated personal and property security activities and incident investigation or custodial activities.
5. Considering the legal regimes, the company chooses security services and creates its own site.
6. The security system can be grouped into specific activities, groups, activity bars or according to the objects (structure).

References

Law of the Republic of Lithuania on Private Detective Activity; TAR, 30-04-2005, No. 6577

Law on Criminal Intelligence of the Republic of Lithuania; State News, 20.10.2012, No. 122-6093

The Code of Criminal Procedure of the Republic of Lithuania; State Gazette, 09-04-2004, No. 37-1341

Law on the Legal Protection of Personal Data of the Republic of Lithuania; State News, 03-07-1996, No. 63-1479

Law on State and Service of Secrets of the Republic of Lithuania; State Gazette, 9-12999, No. 105-3019

Personal And Property Safety Law of the Republic of Lithuania; 2004 m. liepos 8 d. Nr. IX-2327, Vilnius, 1041010ISTA0IX-2327

Burda, R., Krikščiūnas, R., Latauskienė, E., Malevski, H., Matulienė, S. (2004). *Forensic tactics and methodology*. (Kriminalistikos taktika ir metodika). Vilnius

Conklin, J. E. (2004). *Criminology*, 8th ed. Boston: Pearson

Dobryninas, A., Gaidys, V. (2004). *Is it safe for Lithuanian society*? (Experience of victimisation of Lithuanian population and attitudes to criminal justice and public Safety)– the Republic of Lithuania, the Seimas of the United Nations Development Programme. (Ar saugi Lietuvos visuomenė? (Lietuvos gyventojų viktimizacijos patirtis ir požiūris į baudžiamąją justiciją bei visuomenės saugumą) – Lietuvos Respublikos, Seimas Jungtinių Tautų vystymo programa.). Vilnius

Crime threats and human security. (Nusikalstamumo grėsmės ir žmogaus saugumas). Vilnius, 2010

Kormishkina, L. A. (2011). *Methodical instructions on the organization of the self-governing work of course hearings economic safety of the enterprise* (organization). Saransk

Organization of information security (2007). Retrieved form http://www.iso27001security.com/ISO27k_Organization_of_information_security.docx

Software Engineering Institute (2018). Structuring the Chief Information Security Officer Organization. Retvieved form https://www.sei.cmu.edu/

Hayes, B., Kane, G., Kotwica, K. (2013). Corporate Security Organizational Structure, Cost of Services and Staffing Benchmark. Research report. Retrieved from https://doi.org/10.1016/C2012-0-07734-4

About the Author

Rysardas Burda, *Dr. professor*, General Staff Officer
Author is a professor at the Faculty of Law at the University of Kazimieras Simonavičius, working in a key position. Prepared study program “Law and economic security”.
He teaches at the University Bachelor's and Master's Degree Programs the following subjects: criminal procedure law, Criminology, Personal and property law protection, Economic crime investigation.

SECURITY OF SCHENGEN BORDERS

Laura Tarkkanen

Introduction

The free movement of people was already a part of the Treaty of Rome and during the European Economic Community (EEC), the citizens of EEC member states were able to travel freely between the member states. Therefore, it is a natural continuum that the heart of the Schengen area falls under the free movement. The first idea of a united Europe was presented by the former Prime Minister of the United Kingdom – Winston Churchill. He presented the idea right after the war in a famous speech in Switzerland. The founding principle is a united Europe without internal borders and free movement of people and goods. This paper discusses the history of the Schengen area, beginning with the treaty signed by Benelux countries in the 1960s and continuing by presenting the geographic expansion of Schengen area as well as the main measures that are adopted by the countries of Schengen area. The paper also presents how the security of Schengen area is carried out and what is the related legislation in the field of border security. Finally, the paper discusses about the future of Schengen area and presents the up-coming legislation and its impact for the third-country nationals travelling to the Europe.

1. History and development of Schengen

1.1. History of Schengen

The Schengen co-operation can be traced back to an earlier treaty signed by the Benelux countries on 1 July 1960. The Benelux treaty abolished internal border controls and shifts them to the external borders of the Benelux territory. However, the ground for Schengen was established as an intergovernmental cooperation with the signing of the Schengen Agreement in 1985.[383] The Member States: Germany, France, the Netherlands, Belgium and Luxemburg were the first ones to sign the Agreement. The aim of the Agreement was the gradual abolition of controls at the Contracting Parties' common frontiers, to achieve free movement of goods, services and persons, pending provisions adopted by all European Community Member States.[384] Therefore, the Schengen Agreement was signed independently of the European Union, in part owing to the lack of consensus amongst EU member states over whether or not the EU had the jurisdiction to abolish border controls.[385] The Schengen Convention of 1990 is referred to as the implementing instrument of the Schengen Agreement. This Convention contains detailed provisions, which provide the legal base for implementing the general principles first set out earlier in the 1985 Agreement

[383] Kabera Karanja, S. (2008). *Transparency and Proportionality in the Schengen Information System and Border Control Co-operation*. Netherlands: Martinus Nijhoff Publishers, p. 40

[384] Ibid

[385] Craig, P & de Búrca, G. (2003). *EU Law: Text, Cases and Materials*, 3rd Ed. Italy: Oxford University Press, p. 751

document.[386] The compensatory measures which are considered the main features of the Schengen Convention, cover matters of asylum, visa and immigration policy, police co-operation, other forms of co-operation, and the exchange of information both outside and inside the Schengen Information System. The Convention and its main features can be stated to be a ground for the Schengen Area. The Schengen Convention came into effect on 26 March 1995, ten years after it was signed.[387]

The Schengen area represents a territory where the free movement of persons is guaranteed. The signatory states of the agreement have abolished all internal borders in lieu of single external border. Simultaneously, to guarantee security within the Schengen area, cooperation and coordination between police services and judicial authorities have been stepped up. In this case, Schengen cooperation has been incorporated into the European Union (EU) legal framework by the Treaty of Amsterdam of 1997. A protocol attached to the Treaty of Amsterdam incorporates the developments brought about the Schengen Agreement into the EU framework.[388]

1.2. Schengen Acquis

In order to integrate the developments from the Schengen agreement into the EU framework, the Council of the EU had to choose the provisions and measures that formed a genuine *acquis*,

[386] Kabera Karanja, S. (2008). *Transparency and Proportionality in the Schengen Information System and Border Control Co-operation*. Netherlands: Martinus Nijhoff Publishers, p. 41

[387] Ibid, p. 42

[388] EUR-Lex (2009). The Schengen area and cooperation. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=LEGISSUM:l33020

or body of law which could serve as a basis for further cooperation.[389] A list of the elements that make up the acquis, setting out the corresponding legal basis for each of them in the European founding treaties (EC Treaty or the Treaty of the European Union) was adopted by Council Decisions.[390]

2. Security of schengen borders

2.1. Schengen Area

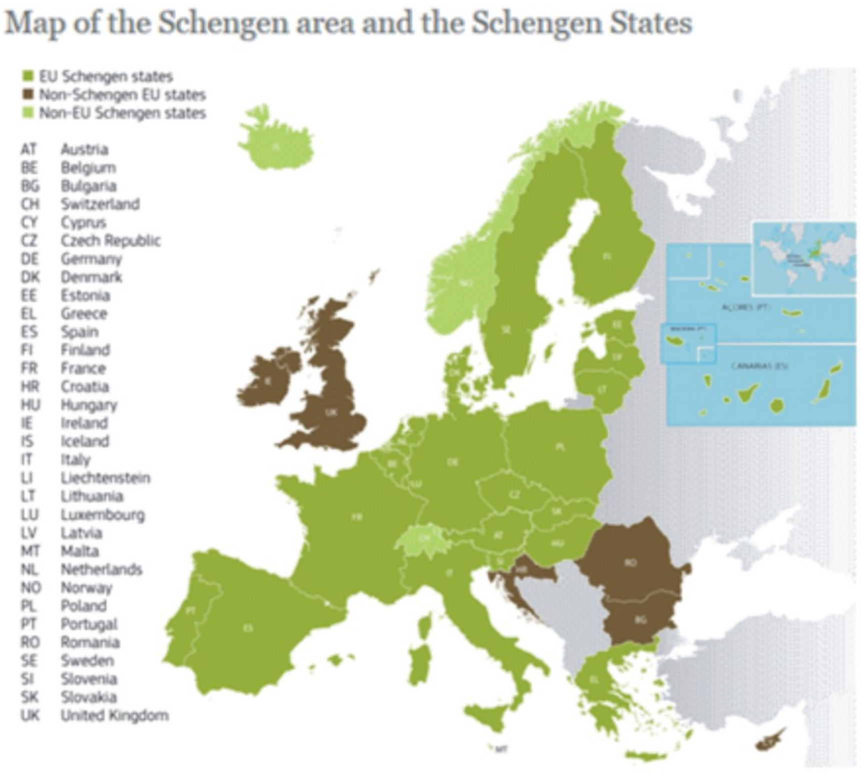
Schengen area includes 26 European countries without internal border controls. Schengen countries include all EU Member States with few exceptional Member States who are not in Schengen as well as four non-EU countries, namely Iceland, Lichtenstein, Norway and Switzerland. However, all countries who are cooperating in European Union are not parties to the Schengen area. Currently, these countries are Bulgaria, Croatia, Cyprus, Ireland, Romania and the United Kingdom. Mainly, either because they do not wish to eliminate border controls or because they do not yet fulfil the required conditions for the application of the Schengen *acquis*.[391] Following picture[392] presents the map of Schengen countries:

[389] EUR-Lex (2009). The Schengen area and cooperation. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=LEGISSUM:l33020

[390] Ibid

[391] Ibid

[392] European Commission. (2018). The Schengen Visa. Migration and Home Affairs. Schengen Information System. Retrieved from https://ec.europa.eu/home-affairs/what-we-do/policies/borders-and-visas/schengen-information-system_en



In addition to the five Member States: Germany, France, the Netherlands, Belgium and Luxemburg, who were the first ones to sign the Agreement in 1985, the Schengen expanded to almost every Member State. Italy signed the agreement on November 1990, Spain and Portugal joined on June 1991, Greece on November 1992, then Austria on April 1995. Northern European countries such as Denmark, Finland and Sweden joined on December 1996, The Czech Republic, Estonia, Latvia, Lithuania, Hungary, Malta, Poland, Slovenia and Slovakia joined on December 2007. Non-European country Switzerland joined on December 2008. Bulgaria, Cyprus and Romania are not yet fully-fledged members of the Schengen area. It means that there are maintained border controls between them and the Schengen area until the EU Council decides the conditions for abolishing internal border controls have been met.[393] The countries that are part of the European Union but have not joined on the Schengen area or have exceptional position, such as the United Kingdom, Ireland and Denmark are discussed later on.

The Schengen countries have abolished checks at the internal borders and created a single external border where immigration checks for the Schengen area are carried out in accordance with identical procedures.[394] Furthermore, common rules regarding visas, right of asylum and checks at external borders were adopted to allow the free movement of persons within the signatory states without disrupting law and order. In order to implement the ground rule of freedom of movement, there was a need to implement compensatory measures as stated above. Compensatory measures involved the improvements regarding the cooperation and coordination between police and the judicial authorities in order to safeguard internal security and also, to fight against the organised crime. For this purpose, the Schengen countries are using the Schengen Information System (SIS) database. The SIS is used by authorities of the Schengen member countries to exchange data on certain categories of people and goods.[395]

[393] EUR-Lex (2009). The Schengen area and cooperation. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=LEGISSUM:l33020

[394] Ibid

[395] Ibid

Measures adopted by the Member States as part of cooperation under Schengen

To summarize, the key rules adopted within the Schengen framework include:

1) removal of checks on persons at the internal borders;
2) a common set of rules applying to people crossing the external borders of the EU Member States;
3) harmonisation of the conditions of entry and of the rules on visas for short stays;
4) enhanced police cooperation (including rights of cross-border surveillance and hot pursuit);
5) stronger judicial cooperation through a faster extradition system and transfer of enforcement of criminal judgments;
6) establishment and development of the Schengen Information System (SIS).[396]

The participation of the countries with exceptional position or the non-EU countries

This chapter explains the participation of the countries which are part of the European Union but have decided to withdraw from the Schengen either from the judicial or practical level. Firstly, Denmark is a part of the European Union and has signed the Schengen Agreement. However, Denmark can choose whether or not to apply any new measures taken under Title IV of the EC Treaty within the EU framework, even those that constitute a development of the Schengen acquis.[397] However, Denmark is bound by certain measures

[396] EUR-Lex (2009). The Schengen area and cooperation. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=LEGISSUM:l33020

[397] Ibid

under the common visa policy.[398] As other exceptions can be mentioned the participation of Ireland and the United Kingdom. The United Kingdom and Ireland are not implementing the measures as part of cooperation under Schengen such as abolishing the internal border checks. However, both countries are cooperating in some aspects of Schengen, namely police and judicial cooperation in criminal matters, the fight against drugs and the SIS. The exceptional position of Ireland and the United Kingdom have stressed the question that the partial participation of these Member States should not reduce the consistency of the acquis as a whole due to the other Member States have been adopting the acquis fully as a basis of the cooperation.

Iceland and Norway belong to the Nordic Passport Union together with Sweden, Finland and Denmark which means that the countries have abolished internal border checks. Iceland and Norway have been actively associated with the development of the Schengen Agreements without voting rights since 1996. Hence, the Council decided to extend Iceland and Norway’s association with the implementation, application and development of the Schengen acquis in 1999. Also, the EU have extended the association to the other non-EU countries such as Liechtenstein and Switzerland in 2008.

2.2. Security of Schengen borders

As mentioned previously, the ground basis for the Schengen area is to abolish internal border checks and create one external border. After signing the Schengen Agreement and adopting it into the EU framework, the Schengen legislation has been developed

[398] EUR-Lex (2009). The Schengen area and cooperation. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=LEGISSUM:l33020

further. Hence, the Schengen Convention has been replaced by new EU legislation; such as Schengen Borders Code. This chapter discusses and describes the nature of the Schengen Borders Code. Furthermore, it presents the developed tools which have a role to reinforce the external borders of the Schengen area. These tools are large-scale IT systems for collecting, processing and sharing information to the external border management. Finally, the chapter presents what the security of Schengen means in terms of different requirements for the third-country nationals. The chapter explains in a practical level how the border crossing for the third country national and EU citizen differs from each other.

Schengen Borders Code – Regulation (EU) 2016/399 – Union Code on the rules governing the movement of persons across borders

As a ground rule, Schengen Borders Code defines that common measures on the crossing of internal borders by persons and border control at external borders should reflect the Schengen *acquis* incorporated in the Union framework, and in particular the relevant provisions of the Convention implementing the Schengen Agreement of 1985. Furthermore, border control is in the interest not only of the Member State at whose external borders it is carried out but of all Member States which have abolished internal border control. Border control should help to combat illegal immigration and trafficking human beings and to prevent any threat to the Member States' internal security, public policy, public health and international relations.[399] Schengen Borders Code defines that border checks should be carried out such a way that they fully

[399] Regulation (EU) 2016/399 of Union Code on the rules governing the movement of persons across borders (Schengen Borders Code). *OJ*, L77, 23.3.2016., p. 6

respect human dignity. Also, border control comprises not only checks on persons at border crossing points and surveillance between those border crossing points, but also an analysis of the risks for internal security and of the threats that may affect the security of external borders.[400] It is therefore necessary to set out the conditions, criteria and detailed rules governing checks at border crossing points and surveillance at the border, including checks in the Schengen Information System (SIS).[401] To emphasise, Schengen Borders Code does not overrule the national law in the external borders. The legislation guides that each Member State should designate the border control tasks in accordance to their national law.

Schengen Information Systems (SIS II)

The Schengen Information System can be presented as a first tool developed to secure the Schengen area. The SIS is one of the measurements adopted by the Member States as a part of the cooperation in the Schengen area. The SIS is a large-scale information system that supports external border control and law enforcement cooperation in the Schengen States. The SIS enables the authorities, for example police and border guards to enter and consult alerts on certain categories of wanted or missing persons and objects.[402] Generally, each alert in the SIS contains information such as name, date of birth, gender, nationality, the reason for the alert and so on. In 2013, the SIS II was launched as an advanced version to replace

[400] Regulation (EU) 2016/399 of Union Code on the rules governing the movement of persons across borders (Schengen Borders Code). *OJ*, L77, 23.3.2016, p. 8

[401] Ibid

[402] European Commission. (2018). Migration and Home Affairs. Schengen Information System. Retrieved from https://ec.europa.eu/home-affairs/what-we-do/policies/borders-and-visas/schengen-information-system_en

the current system (SIS). The SIS II enables for example the possibility to use biometrics and a facility for direct queries on the system. Overall, the main purpose of both versions of SIS (I & II) during the recent years have been to help preserve internal security in the Schengen area due to the absence of internal border checks. Currently, the SIS II operates in 26 Member States and four associated countries, such as Switzerland, Norway, Liechtenstein and Iceland. As Bulgaria, Romania and Cyprus are not fully part of the Schengen area, there are some restrictions regarding their use of Schengen-wide SIS alerts. Also, as explained previously, the United Kingdom has been accessed to SIS as a non-Schengen country, however, the United Kingdom cannot issue or access Schengen-wide alerts for refusing entry or stay into the Schengen area. Furthermore, Ireland is carrying out preparatory activities to connect to the SIS, but it has the operational capabilities as the United Kingdom. Cyprus has a temporary derogation from joining the Schengen area and is not yet connected to the SIS.[403]

Visa Information System (VIS)

The Visa Information System (VIS) allows Schengen States to exchange visa data. The VIS consists of a central IT system and of a communication infrastructure that links this central system to national systems.[404] VIS connects consulates in non-EU countries and all external border crossing points of Schengen countries. It processes data and decisions relating to applications for short-stay

[403] European Commission (2018). Migration and Home Affairs. Schengen Information System. Retrieved from https://ec.europa.eu/home-affairs/what-we-do/policies/borders-and-visas/schengen-information-system_en

[404] Ibid

visas to visit or to transit through the Schengen area.[405] The main purpose of VIS is to enable border guards to verify that a person presenting a visa is its rightful holder and to identify persons found on the Schengen territory with no or fraudulent documents.[406] Hence, visas include biometric data as it allows the border guard to confirm a visa holder's identity with an accurate and secure check. Consequently, Schengen Borders Code states that since only verification of fingerprints can confirm with certainty that a person wishing to enter the Schengen area is the person to whom the visa has been issued, provision should be made for the use at external borders of the Visa Information System (VIS).[407]

2.3. Security of Schengen Borders in practise

The border crossing in the Schengen borders may include different kind of processes whether the traveller is an EU citizen or a third country national. This paragraph presents the difference between an EU citizen crossing the border comparing a third-country national crossing the same Schengen border. This paragraph explains what kind of different actions should be considered or taken care of by a traveller before entering to the border. Furthermore, what is the difference between the different border checks for an EU citizen and a third-country national? In this case, a third country national is defined to be "any person who is not citizen of the European Union within the meaning of Art. 20 (1) of

[405] European Commission (2018). Migration and Home Affairs. Schengen Information System. Retrieved from https://ec.europa.eu/home-affairs/what-we-do/policies/borders-and-visas/schengen-information-system_en

[406] Ibid

[407] Regulation (EU) 2016/399 of Union Code on the rules governing the movement of persons across borders (Schengen Borders Code). *OJ*, L77, 23.3.2016., p. 10

Treaty of Funding the European Union and who is not a person enjoying the Union right to free movement, as defined in Art. 2(5) of the Schengen Borders Code."[408] According to this definition, nationals of Norway, Iceland, Liechtenstein and Switzerland are not considered as third country nationals.

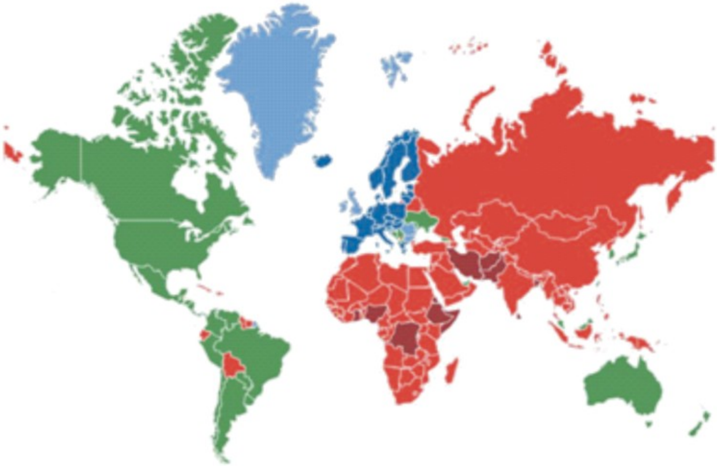
Council Regulation (EC) No 539/20017 lists the third countries whose nationals must be in possession of visas when crossing the external borders and those whose nationals are exempt from that requirement. However, if a short-stay visa is issued by any of the Schengen countries, the visa holder is entitled to travel throughout the 26 Schengen countries. Hence, the traveller group whose nationals must be in possession of visa is called visa holder and those whose nationals' visa is not required are called as visa exempt.

The picture[409] (next page) below illustrates the visa requirements. The countries marked in:

1) blue colour are part of Schengen or EU States and territories of EU not part of Schengen and other expectations;
2) red colour are the visa required countries;
3) green colour are no visa required (visa exempt) countries.

[408] European Commission (2018). Migration and Home Affairs. Schengen Information System. Retrieved from https://ec.europa.eu/home-affairs/what-we-do/policies/borders-and-visas/schengen-information-system_en

[409] European Commission (2018). Visa Policy. Migration and Home Affairs. Schengen Information System. Retrieved from https://ec.europa.eu/home-affairs/what-we-do/policies/borders-and-visas/schengen-information-system_en



While 'minimum checks' are performed on EU citizens and persons enjoying the right of free movement, third country nationals crossing the Schengen area external borders are subject to ‘thorough checks’ made manually by the border guards at the borders (both at entry and exit). As a general rule, third country nationals have the right to enter for a short stay of up to 90 days within any 180 day period. Currently the stamping of the travel document indicates the dates of entry and exit is currently the only available method to border guards and immigration authorities to calculate the duration of stay of third country nationals as well as to verify if someone is overstaying their stay in Europe. These stamps can be difficult to interpret: they may be unreadable or the result of counterfeiting. Similarly, it is difficult for consulates to process visa applications to establish the lawfulness of previous visas on the basis of stamps present in the travel document. As a result the whole procedure may be considered as problematic and always not systematically implemented.

Ensuring systematic and reliable identification of overstayers

Irregular immigrants include both persons who crossed the borders irregularly – usually not at an official border crossing point and the so called "overstayers": persons having legally entered the EU at an official border crossing point but who stayed after their entitlement to do so expired. The Entry/Exit System (EES) addresses this category of irregular migration and the issue is explained later in this article. Due to the border crossings by third country nationals are not currently registered into any ICT system, there is no possibility to establish lists of overstayers.

3. Future of Schengen area

3.1. Smart Borders

The Smart Borders Package was proposed by the Commission in February 2013. It aims to improve the management of the external borders of the Schengen Member States, borders of the Schengen Member States, fight against irregular immigration and provide information on overstayers, as well as facilitate border crossings for pre-vetted frequent third country national (TCN) travellers.[410] The Smart Borders Package suggested the establishment of an Entry/Exit System (EES) and a Registered Traveller Programme (RTP). However, the Council and the European Parliament stated technical, operational and cost concerns in 2014 which were mainly related to the overall feasibility of the proposed new systems and some of the features. In order to further assess the technical, organisational and financial impacts of the various possible ways to

[410] European Commission (2018). Migration and Home Affairs. Schengen Information System. Retrieved from https://ec.europa.eu/home-affairs/what-we-do/policies/borders-and-visas/schengen-information-system_en

address the concerns, the Commission initiated a proof of concept exercise consisted of two stages.[411]

The first stage included a commission-led Technical Study which identified and assessed the most suitable and promising options and solutions. Second stage included a testing phase entrusted to the Agency for the Operational Management of large-scale IT Systems in the area of Freedom, Security and Justice (eu-LISA) aimed at verifying the feasibility of the options identified in the Technical Study and validating the selected concepts for both automated and manual border controls.[412] There has been a question regarding the reversibility in the growing reliance on data and information exchange schemes for the conduct of the European Union's Justice and Home Affairs policies. According to Vasile[413] the question of whether or not past policy options are reversible were in the central in the debates surrounding this policy domain which had been characterised over the past few years by a steady flow of proposals aiming at establishing new large-scale systems for law enforcement purposes. Smart Borders' testing phase took place in 12 countries in 18 air, sea and land border crossing points and involved nearly 58 000 third country nationals and about 350 border guards.[414] On that basis, the Commission adopted a legislative proposal for Smart Borders on 6 of April, 2016. The revised legislative

[411] European Commission (2018). Migration and Home Affairs. Schengen Information System. Retrieved from https://ec.europa.eu/home-affairs/what-we-do/policies/borders-and-visas/schengen-information-system_en

[412] Ibid

[413] Vasile, S. (2014). The "Smart Borders Package" and the improvement of the management of the external borders of the Schengen Area. *Journal of Criminal Investigations*, No. 7 (1), p. 74

[414] European Commission (2018). Migration and Home Affairs. Schengen Information System. Retrieved from https://ec.europa.eu/home-affairs/what-we-do/policies/borders-and-visas/schengen-information-system_en

proposal for Smart Borders includes a Regulation for the establishing of an Entry/Exit System and a proposed amendment to the Schengen Borders Code to integrate the technical changes needed for the Entry/Exit System. The European Parliament adopted the Commission's proposal in October 2017. Hence, the final text will have to be adopted by the Council. After that, the development of the system is expected to start with a view to having it operational by 2020. The next paragraph explains the Entry/Exit System more thoroughly as it will have a key role by securing the Schengen borders in the near future.

3.2. Entry/Exit System

Generally, Entry/Exit System (EES) is a database which records the name, type of travel document, biometrics and the information on the time and place of entry and exit of third country nationals entering the Schengen area. It modernises external border management by improving the quality and efficiency of controls as well as the detection of document and identity fraud. The system will apply to all non-EU nationals who are admitted for a short stay into the Schengen area (maximum 90 days in any 180-days period). The legislative proposal for the EES explains that it will facilitate the border crossing by addressing the following challenges.

1. Addressing border check delays and improving the quality of border checks for third country nationals.

   For this challenge, the introduction of the EES will ensure:

   - precise information, rapidly delivered on demand to border guards during border checks, by replacing the current slow and unreliable system of manual stamping of passports; this will allow for both a better monitoring of the authorised stay as well as more efficient border checks;

- information to border guards on refusals of entry of third country nationals and will allow for refusals of entry to be checked electronically in the EES;
- precise information to travellers on the maximum length of their authorised stay;
- possibility for automated border controls for third country nationals under the supervision of the border guards in accordance with the conditions foreseen in the revised proposal to amend the Schengen Borders Code.[415]

2. Ensuring systematic and reliable identification of 'overstayers'.

As an overstayer can be considered a person who has been legally entered the EU at an official border crossing point but who stayed after their entitlement to do so expired. As the third country nationals are not registered in any system, there is no possibility to establish any lists of overstayers.

For this challenge, the EES will introduce:

- provide precise information on who is overstaying their authorised stay, which will support controls within the territory and allow to apprehend irregular migrants more efficiently;
- support the identification of irregular migrants; by storing biometrics in the EES on all persons not subject to the visa requirement, and taking into account that the biometrics of visa holders are stored in the VIS, Member States' authorities will be able to identify any undocumented

[415] Proposal for a regulation of the European Parliament and of the Council establishing an Entry/Exit System (EES) to register entry and exit data and refusal of entry data of third country nationals crossing the external borders of the Member States of the European Union and determining the conditions for access to the EES for law enforcement purposes and amending Regulation (EC) No 767/2008 and Regulation (EU) No 1077/2011. 2016/0106 (COD)

irregular migrant found within the territory that crossed the external border legally; this will in turn facilitate the return process;

- allow for an evidence-based approach through the analysis generated by the system. In the case of visa policy for instance, the EES will provide precise data on whether there is problem with overstayers of a given nationality or not, which would be an important element when deciding whether to impose or lift visa obligations on a third country in question.[416]

3. Reinforcing internal security and the fight against terrorism and serious crime.

   Controls of third country nationals at external borders involve identity checks and searches against various databases of known persons or groups posing a threat to public security that should be either apprehended or denied entry to the territory. However, if a third country national destroys his/her official documentation once inside the Schengen area, it can be very difficult for law enforcement authorities to identify that person in case he/she is suspected of a crime or is a victim of crime.[417]

[416] Proposal for a regulation of the European Parliament and of the Council establishing an Entry/Exit System (EES) to register entry and exit data and refusal of entry data of third country nationals crossing the external borders of the Member States of the European Union and determining the conditions for access to the EES for law enforcement purposes and amending Regulation (EC) No 767/2008 and Regulation (EU) No 1077/2011. 2016/0106 (COD)

[417] Ibid

For this issue, the introduction of EES will:

1) support the reliable identification of terrorists, criminals as well as of suspects and victims;
2) provide a record of travel histories of third country nationals including crime suspects. It would complement the information available in the Schengen Information System.[418]

Conclusions

1. Legislation constitutes the common framework for the security of Schengen Borders.
2. Security of Schengen borders is practically carried out by using common ICT systems such as SIS II and VIS.
3. Smart Borders against irregular immigration, overstaying of visas and also facilitating the border crossings fort third-country nationals.

In order to conclude the topic – the security of Schengen borders, it is necessary to look back what is the main principle of the Schengen area. Within this case, shall be kept in mind the political framework of European Union. This framework is based on the free movement of people and goods in Europe without internal borders. Schengen Area can be described as a tool to fulfil this political goal. Consequently, to achieve the goal, the progress to

[418] Proposal for a regulation of the European Parliament and of the Council establishing an Entry/Exit System (EES) to register entry and exit data and refusal of entry data of third country nationals crossing the external borders of the Member States of the European Union and determining the conditions for access to the EES for law enforcement purposes and amending Regulation (EC) No 767/2008 and Regulation (EU) No 1077/2011. 2016/0106 (COD)

build up the European Union and its main principles was started with the Treaty signed by the Benelux countries on the 1960s.

The main measures as a part of Schengen cooperation are removal of checks on persons at the internal borders, a common set of rules applying to people crossing the external borders of the EU Member States, harmonisation of the conditions of entry and of the rules on visas for short-stays, enhanced police cooperation, stronger judicial cooperation through a faster extradition system and transfer of enforcement of criminal judgments as well as establishment and development of the Schengen Information System. As mentioned the main principle of Schengen area lays on the idea of no internal borders which has to be followed by each Member State. However, as discussed earlier, there are few exceptions what are accepted to be a part of Schengen despite of that they are not part of European Union. Also, as mentioned, the European Union countries, such as the United Kingdom and Ireland have been withdrawn from the Schengen despite their participation in European Union.

In order to conclude how the Schengen Area is managed, we need to examine the legal ground of it. Schengen Borders Code is a legal basis for all activities executed within the Schengen area. Can be stated that the Schengen Borders Code is the cornerstone for national legislations and Schengen countries apply the legislation accordingly. Regarding the tools of managing the Schengen area, they fall into the ICT systems such as Schengen Information System (SIS) and Visa Information System (VIS). As stated, there are no law enforcement authorities physically guarding in the European borders, they are fulfilling their task of protecting national security by ICT systems and profiling the risk groups.

As discussed earlier, the future of Schengen area will change as the legislation for the third-country nationals travelling to and from Europe is going to be changed in order to enable the faster border crossings. The legislation package, Smart Borders, is introduced and the Entry–Exit System (EES) will be in operational use in 2020. With Smart Borders legislation package, the Schengen Area prefers to fight against irregular immigration and provide information of overstayers as well as facilitate border crossings for pre-vetted frequent third-country national travellers.

The original idea of Schengen was a tight area of six founding European countries. It also had a symbolic value because Germany, France and the Benelux countries were cooperating since Second World War However, today, Schengen area has expanded geographically quite widely and the external border of Europe is expanding close to the Arabic and Asian countries, Belarus and Russia. Mentioned countries may have had issues related to security, such as conflicts, terrorisms and refugee issues. Therefore, the challenges for managing and securing the Schengen area have been growing exponentially. Furthermore, it shall be kept in mind that the mutual understanding of the principles of the Schengen area has been recently differentiating within the European Union. For example, due to the refugee crisis, some of the Schengen countries carried out internal border checks within their own borders. Eventually, if European Union wants to develop and improve Schengen area, Union shall consider to include different policy making actions with Europe’s neighbour countries. All in all, Schengen area with its constraints has been a success story. It has answered successfully to the challenges of geographical and functional expansion. Furthermore, it has been able to define the clear measures for cooperation in the Schengen area. Consequently, the key factor to the successful execution of Schengen area has been the capability of European Union for further developing with new tools and legislation. Thus, the Schengen area's expansion to the new countries of European Union has been carried out successfully. All in all, the above mentioned actions can be concluded as a good path that shall be followed in the future.

References

Craig, P & de Búrca, G. (2015). *EU Law: Text, Cases and Materials*, 6th Ed. Italy: Oxford University Press, p. 1159

Craig, P & de Búrca, G. (2003). *EU Law: Text, Cases and Materials*, 3rd Ed. Italy: Oxford University Press

Kabera Karanja, S. (2008). *Transparency and Proportionality in the Schengen Information System and Border Control Co-operation.* Netherlands: Martinus Nijhoff Publishers, p. 466

Vasile, S. (2014). The "Smart Borders Package" and the improvement of the management of the external borders of the Schengen Area. *Journal of Criminal Investigations 2014,* 7 (1), pp. 73–78

European Commission (2018). Migration and Home Affairs. Schengen Information System. Retrieved from https://ec.europa.eu/home-affairs/what-we-do/policies/borders-and-visas/schengen-information-system_en

European Commission (2018). Migration and Home Affairs. Smart Borders. Retrieved from https://ec.europa.eu/home-affairs/what-we-do/policies/borders-and-visas/smart-borders_en

European Commission (2018). Migration and Home Affairs. Visa Information System (VIS). Retrieved from https://ec.europa.eu/home-affairs/what-we-do/policies/borders-and-visas/visa-information-system_en

European Parliament and Council Regulation 2016/399 (9th March 2016) on a Union Code on the rules governing the movement of persons across borders. *OJ*, L77, 23.3.2016

EUR-Lex. (2009) The Schengen area and cooperation. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=LEGISSUM:l33020

European Parliament and Council Proposal amending Regulation no 767/2008 and Regulation No 1077/2011 (6th April 2016) on Proposal for a regulation of the European Parliament and of the Council establishing an Entry/Exit System (EES) to register entry and exit data and refusal of entry data of third country nationals crossing the external borders of the Member States of the European Union and determining the conditions for access to the EES for law enforcement purposes. 2016/0106 (COD)

About the Author

Laura Tarkkanen, Project Manager, Bachelor of Business Administration (Security Management) – Laurea University of Applied Sciences. Undergraduate in Bachelor of Arts (Law), Tallinn University.
Author has worked as a project manager in several R&D projects with various funding instruments since 2012. Ms. Tarkkanen has managed several border security related projects such as Automated Border Control Gates for Europe (ABC4EU) and Cross-Border Photonics Initiative (CBPI). Her expertise is in border security and applying service design approach into border security research. In border security research, she has worked in successful collaboration with cross-sectoral actors such as authorities, industry and academia. Ms. Tarkkanen has published several scientific publications from the previous projects.

VIDEO SURVEILLANCE SYSTEMS

Vilnis Veinbergs
Dainis Siliņš

Introduction

Public and individual security is becoming more topical by the day. This is true not only due to the fact that local criminal elements try to steal or do another type of damage to owners, but also because our security is largely affected by the global development tendency towards a complete and instantaneous circulation of information by means of the world wide web, cross-border cooperation of sovereign states and commerce, the movement of people across the borders of various unions and, for instance, the free flow of people in the EU area, etc. This kind of "freedom" raises a multitude of different issues to the security staff in terms of how to protect the assets or, if necessary, how to detain persons.

Top managers of organizations created to perform the generalised or special type of activities, internal security services and commercial guarding operators must understand the essence of security and the degree of necessity for its preventive actions, which substantially increases or decreases financial spending on security measures. This means that there is a need for complete analysis of the existing risks and threats at each protected object, including analysis of the technical means required, guarding and protection tactics applicable, the conditions limiting or improving security, the factors, which provide an opportunity for preventive measures for limiting or minimising the consequences of illegal actions, their damage to property and human health.

This means that thinking about security measures no longer falls solely into the realm of security staff responsibility. All of us, each member of society must be aware of the existing risks and possible consequences resulting from neglecting them.

One can take care of the security of property and people by employing various technical means, which is cheaper compared to maintaining outposts of physical persons. They can also prove to be more effective in comparison with the natural flaws inherent in human beings.

Technical means used for guarding purposes are employable both as integrated in a common security system, which includes separate mechanisms, equipment and systems – guarding alarms; fire alarms, video surveillance systems; access control systems, notification systems, as well as separately by using a designated video surveillance camera, which delivers a signal to the receiver via the world wide web or by means of a video surveillance system.

Video surveillance is one of the key instruments for performing guarding operations, because:

1) it can be used preventively by warning a criminally-minded individual of the fact that his/her activities are being monitored or recorded, thus containing that person from illegal actions;
2) the protected object is under surveillance in real time and the reaction to an illegal activity can take place momentarily;
3) the obtained video surveillance data are recorded and are usable for disclosing an illegal activity, for investigation of consequences, as evidence in the court of law as well as for the analytical work related to ensuring the security of a protected object.

The historically known beginnings of visual surveillance date back already to the 19th century, when prison staff had to provide increased attention to preventing prisoners from leaving the territory of detention facilities. They used photographic cameras employing quite expensive silver-based materials and performed analytical work on the escape methods of prisoners.[419]

However, the beginnings of the video camera used for data collection are related to the development of television and shooting of its footage. The television equipment had been built in for the 1940 Olympic Games that were to be held in Tokyo and which had been cancelled due to the start of World War II.[420] In August 1940 RCA discussed with Richard C. Tolman its idea of a television-equipped radio-controlled aerial torpedo. RCA (Radio Corporation of America) felt competent to undertake the television development but was not equipped to investigate the aerodynamic aspects.[421] In 1941 a team was led at Peenemünde in developing and installing a closed-circuit television system to give low-risk monitoring of the rocket launches. A two-camera system was installed at the launch pad to relay live pictures by cable to a control room 2.5 km away. One of the compact cameras had a telephoto lens and the other a wide-angle lens, and one of them had to be replaced after being destroyed when the first V2 rocket blew up. There is a view that the first video camera was developed at Siemens AG by a German engineer Walter Bruch. That camera was displayed at an exhibition

[419] Caputo, A. C. (2014). *Digital video surveillance and security*. 2nd ed. Elsevier inc., pp. 2–4

[420] Abramson, A. (2007). *The History of Television 1942 to 2000*. McFarland & Co Inc (Verlag), pp. 3–7

[421] Ibid

centre in 1942.[422] It is apparent that the use of video cameras for various surveillance purposes already dates back to the middle of the 20th century and since then it has increasingly proven its necessity. With a growing demand, the science and research allocated significant time and effort to improving video surveillance cameras and their systems. Today we speak not only about analogue cameras but also about the improvement of digital cameras and their rapid technical development is evident in the World Wide Web and in specialised literature. New video camera solutions are being offered globally and can be viewed at various exhibitions devoted to security. It is no longer an equipment designed solely for undercover surveillance used by security services. It is a high-tech equipment of various sizes, adaptable to the environment and with varied resolution and filming angle for obtaining data, with various types of connecting cables or operating wirelessly.

Video surveillance has become an inevitable daily companion. Therefore, when starting to choose a video surveillance system, one should always assess its necessity, consider the type of equipment required, and whether cameras will provide the quality required for their purpose, etc. The choice of a surveillance angle (for obtaining data) is key to choosing the right camera, since it has to comply with normative acts, regulating personal privacy. Video surveillance is not acceptable in places where physical persons expect a particularly high level of privacy protection, for instance, in recreation areas of workplaces (and even at workplaces an employee has a right to the inviolability of his/her private life), in fitting rooms of stores as well as in toilets. This means any information in respect to an identified or identifiable physical person.

[422] Abramson, A. (2007). *The History of Television 1942 to 2000*. McFarland & Co Inc (Verlag), pp. 15–19

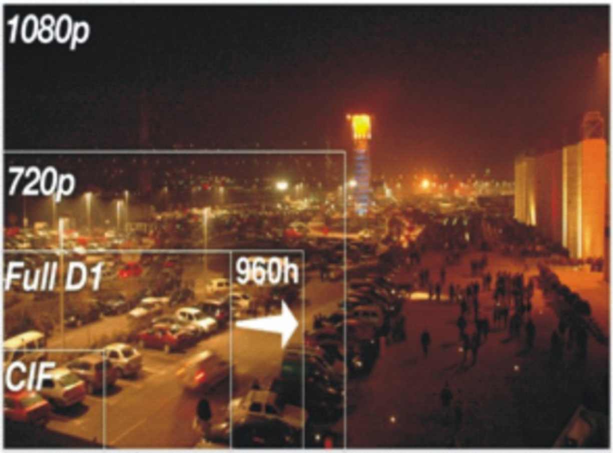
1. The specific characteristics of video surveillance

The contemporary video surveillance equipment market is saturated with various technical video surveillance solutions. It is difficult for a non-expert to choose a video camera or a system which would be most suitable for meeting a surveillance goal. Thus, it is necessary to assess the required necessities and possibilities, be it financial or related to a possible placement of cameras for local use or linked with the security aspects of cameras themselves, et al.

Similarly to other areas of technology, video cameras and their possibilities are developing rapidly. Therefore, it is virtually impossible to single out or recommend anything in terms of their technical data or characteristics features. Something that represents a cutting-edge innovation today may be an outdated technology already in one year's time. A modern video surveillance system equipment provides for the use of digital information transmission and storage technologies. Such video surveillance systems provide for their connection with computers and software sets. Thanks to the technical progress, it is possible to conduct surveillance of an object from anywhere in the world with an access to the global Internet.

It should be taken into account that the quality of the obtainable picture is one of the most important aspects of video surveillance.

When assessing the kind of video surveillance system is most purposeful for the needs of a particular surveillance work, it is necessary to clarify the required picture quality. Whether there is a need for a minute and detailed information on the picture for further analysis or it would be sufficient to have a general view, without small visible details, like people's faces, car number plates, etc. It is also possible that the whole video surveillance system would have to be formed the way that it would require placement of high-resolution cameras with high-quality picture reception in some spots, while other locations would require lower resolution images. Resolution is indicated by the number of pixels (nominal dots) on a computer screen, usually stating the width and the height with units in pixels, for instance, “1024×768”, where 1024 pixels indicate the width, while 768 pixels indicate the height. Picture 1 contains a vivid example of various pixel size indicators. An equal quality image is seen only upon observing the area seen in the monitor if the area reflected in the monitor is zoomed in, the quality of the picture loses its sharpness, becoming blurry and without precise contours (Picture 2).



Picture 1. **Visualisation of video surveillance resolution standards**[423]

[423] SIA EMEM (2007). Video Surveillance Resolution CIF/D1/960H/720p/1080p Difference and Comparison with Different Standards. Retrieved from http://www.vns.lv/index.php?aux_page=aux24

The more pixels are available, the higher the quality of the receivable picture. It should be noted that cameras with an identical number of pixels, but with a different reception angle, will produce a different picture quality. Under the condition that the number of pixels at a wider or narrower angle is constant, the narrower the angle, the higher the picture quality.

2. Types of video surveillance systems

Video surveillance system – a set of technical equipment designated for the surveillance of an object. Video surveillance systems consist of a camera or a number of cameras, a data transmission installation, a recording device and a monitor for viewing and analysis of data. It should be taken into account that video surveillance can take place constantly or depend on the time schedule set-up, or a recording can take place only in case of action in the selected surveillance area, for instance, movement, accumulation of smoke, sharp changes in temperature, etc. data obtained as a result of video surveillance can be recorded in a recording device and they can also be viewed in real time without making a recording. However, taking into account that video surveillance is not just a preventive action, it is recommended to record all video data in the recording devices in order to use them upon necessity (investigation, clarification of circumstances, etc.). The transmission of a signal or data, in their own turn, are divided into wired and wireless systems. There are two types of video systems available nowadays – analogue and digital or IP systems. Analogue systems are more widespread.

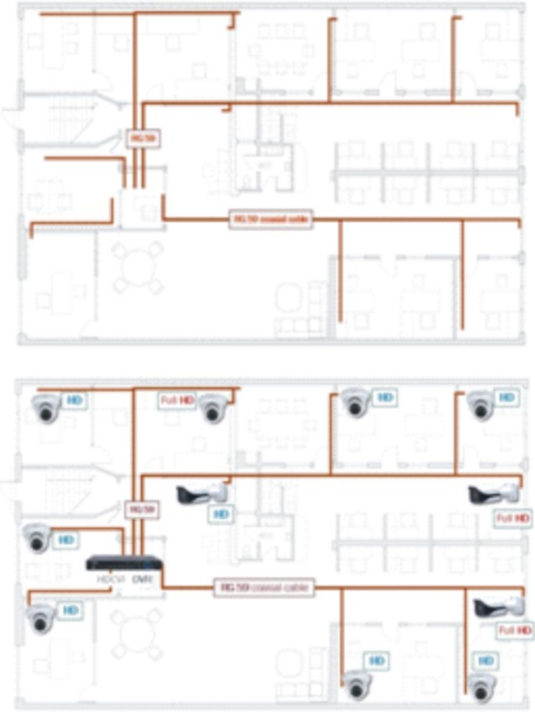
2.1. Analogue systems

Both IP and analogue video surveillance systems are available for the purposes of guarding operations. Thanks to the high quality of images provided by the IP systems, these systems started to replace the analogue ones. However, upgrades of analogue systems returned to the market in 2016 in the form of HDI CVI and AHD technologies, providing data quality, which is similar to IP systems.

The new analogue video surveillance technologies provide 720p and Full HD 1080p resolutions, which is equal to the quality provided by digital IP systems. Moreover, the costs of using the new analogue systems are substantially lower compared to the digital video surveillance systems. Thus, price wise it is closer to analogue cameras, while its resolution is similar to IP and HD SDI cameras. Furthermore, their installation is made simpler by the fact that the for the connection purposes of the new analogue video systems one can make use of the traditional analogue connectors and coaxial cables. When installing a new high-resolution video surveillance system, one uses the existing analogue system cables, thus increasing the resolution up to 2 Mp (Picture 2, next page).

The possibility of using a remote parameter adjustment for many HD CVI technology camera systems provides a substantial convenience from a user perspective. This function is useful since it provides an opportunity to adjust the camera for specific conditions and in line with the purposes of its use from home, office or anywhere else with an access to the global network. It is more convenient to configure picture quality exactly at the offset of the most complicated weather conditions: night, fog, backlighting. It is also possible to control cameras remotely with a help of a motorised directional and zooming function (PTZ).[424]

[424] SIA Drošībai.lv (2018). Analogās AHD kameras un DVR. Retrieved from http://www.drosibai.lv/video-noverosana/ahd-kameras-un-dvr



Picture 2. **The previously installed and used coaxial cable installation (on the top), which works as the basis for installing HD and Full HD 1080p HD CVI camera system (in the bottom)**[425]

AHD (analogue high definition) is another of the new analogue HD video technologies, which can serve as an alternative to digital. It provides a high analogue resolution of 1280×720 or 1 megapixel.

The advantages of AHD, compared to the old generation analogue systems:

1) supports up to 960H Analogue, 720p AHD cameras;

[425] SIA Drošībai.lv (2018). Explanation of video surveillance. Retrieved from http://www.drosibai.lv/video-noverosana/skaidrojumi-par-videonoverosanu

2) transmits with zero latency over standard coaxial cabling (smooth motion);
3) backwards compatible with all analogue cameras and standard coaxial cabling;
4) features digital zoom capabilities in both live and playback mode;
5) hybrid recorder accepts select standard definition analogue (CIF-960H), and like-branded AHD (720p) cameras, in limited configurations.[426]

2.2. IP or digital surveillance systems

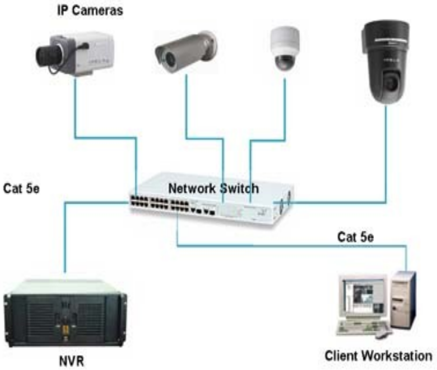
As it was already described in the previous chapter, HD CVI analogue cameras serve as an alternative to the IP (Internet protocol) cameras, which are becoming increasingly popular among those engaged in guarding operations. However, IP cameras nowadays grow in popularity and applicability. Even despite the fact that the use of IP camera video surveillance systems is considerably more expensive. There is a question, why?

In distinction with the aforementioned standards, the main function of an IP (Internet protocol) camera is to provide a remote video transmission via a computer network. Therefore, IP cameras use a computer network for data signal transmission. This device includes a high-quality digital video camera and simultaneously works as a network server providing access to this camera and allowing to perform video surveillance from any computer at any place by means of a global or a local network of a company. This explains the popularity of IP video systems. In order to install this type of video surveillance system, it is not always necessary to

[426] HD Analog.com (2015). AHD CCTV Technology Commonly referred to as: AHD, Analog HD. Retrieved from http://www.hdanalog.com/options/ahd.html

create a separate cable network. Any contemporary office building, educational institution, merchant store and other places have its own data transmission network, which can be used for the transmission and reception of IP video system data.

The second reason for the popularity of IP cameras due to be mentioned is their high resolution. IP cameras have powerful processors, allowing them to operate as small computers. This technology provides an improved image quality, coding and compressing of video as well as ensures data analysis and smart management of the video surveillance process. The operation of IP camera device is simple, offering many options, since the use of remote global network access provides for watching videos online, gives access to the recording archive and allows to configure device parameters. For the recording of videos, IP cameras use NVR (network video recorder) or computers equipped with specialised video surveillance software (Picture 3).

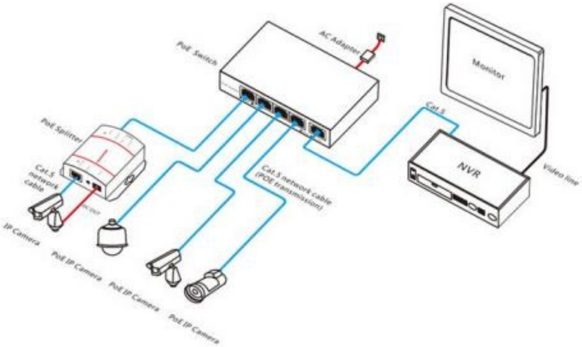


Picture 3. **IP video surveillance system**[427]

[427] SIA Drošībai.lv (2018). Explanation of video surveillance. Retrieved from http://www.drosibai.lv/video-noverosana/skaidrojumi-par-videonovroanu

2.3. PoE technology

PoE is the most commonly used technology for setting up an IP camera video surveillance system. This involves using simplified camera connection since video and data streaming, as well as power supply, is provided via a single connection (Picture 4).



Picture 4. **Placement of PoE connection in an IP video surveillance system**[428]

The feeding of PoE (Power over Ethernet) through Ethernet. In other words, a single cable of a computer network provides the flow of data and the flow of power.

The creation of a PoE connection in a standard network is quite simple. In order to connect a single PoE device, it is possible to use a PoE injector, while for the connection of multiple devices one should use a network switch with PoE capability.

[428] Shenzhen MVTEAM Technology Co., Ltd. (2018). What's the relative merits of transmission modes (POE,EoC,PLC) for CCTV System? Retrieved from https://www.mvteamcctv.com/news/What-s-the-relative-merits-of-transmission-modes-POE-EoC-PLC-for-CCTV-System.html

Some of the key advantages of an IP camera compared to analogue cameras include:

1) remote administration from any location;
2) digital zoom;
3) the ability to easily send images and video anywhere with an Internet connection;
4) progressive scanning, which enables better quality images extracted from the video, especially for moving targets;
5) adjustable frame rates and resolution to meet specific needs;
6) two-way communication;
7) the ability to send alerts if suspicious activity is detected;
8) lower cabling requirements;
9) support for intelligent video.[429]

2.4. Wireless video surveillance

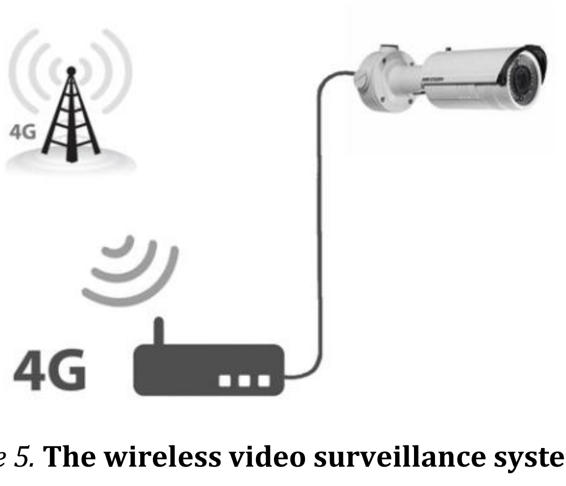
Wireless video surveillance is a type of video surveillance, which nowadays, thanks to the availability of mobile internet, is gaining increased popularity. This type of video surveillance does not require cable connection with a recording device and a monitor. Successful operation of the system requires the presence of a sufficient flow of mobile data.

Taking into account the development of mobile internet provision over the past few years and the availability of 4G mobile practically everywhere, wireless video surveillance systems are

[429] TechTarget (2010). IP camera. Retrieved from https://whatis.techtarget.com/definition/IP-camera

being increasingly used. They are used in order to provide a twenty-four hour external and internal surveillance at various objects. It is possible to install wireless video surveillance systems in a block of flats, a single flat, in public buildings and at production facilities, even in the wild outdoors for monitoring nature development and bird nesting. Wireless surveillance systems are proving effective for the use in large buildings without a local computer network, in large territories, for instance, parking lots, where installing of cables by air or under the ground would be costly and complicated. A wireless video surveillance set is simple and consists of wireless video cameras equipped with Wi-Fi receivers, a video signal receiver and a monitor (Picture 5).

Moreover, nowadays any smart device can be used as a monitor making video surveillance even more effective and with a broad range of possibilities.



Picture 5. **The wireless video surveillance system**[430]

[430] SIA Drošībai.lv (2018). Explanation of video surveillance. Retrieved from http://www.drosibai.lv/video-noverosana/skaidrojumi-par-videonovroanu

Providing of wireless video surveillance requires a relatively sizeable flow of mobile data. Thus, the main parameters of choice that should be taken into account include:

1) internet speed. It should be noted that upload speed is the most important requirement of video surveillance, since, once connected, the camera sends video data over the Internet. The upload speed is typically 3 times slower compared to the download speed. For instance, if the speed of download is 4 Mbs, the upload speed will be in the 1.2–1.6 Mbs range;
2) the planned data transmission volume at the moment of connection. One should understand the volume of video data flow. It is directly dependant on the video resolution, compression and filming intensity (frames per second). Different systems are used for compression and coding. It can be exemplified by H.264 video compression system, which is the most frequently used and most suitable;
3) the choice of a modem and/or a router. Providing video surveillance requires both: a mobile modem and a router. Mobile network operators provide an already joint modem and router devices;
4) a fixed IP address. Up to this moment, the specifics of the internet commutation determine that the operation of video surveillance requires a fixed or static IP address.

3. Comparison of video surveillance systems

Nowadays, when planning the creation of a video surveillance system, difficulties can be posed by the necessity to choose between different technologies. When making a choice, it is recommended to evaluate the most appropriate camera and consequently: the parameters offered by various video surveillance systems. A comparison of the most popular contemporary video surveillance devices is shown in Table 1.

Table 1

Comparison of video surveillance systems[431]

	Analogue	**AHD**	**HD CVI**	**HD TVI**	**IP cameras**
Resolution	CIF	HD 702p	HD 720 and 1080p	HD 720 and 1080p	HD 1080p
Pixels	704×576 0.4 Mpix	1280×720 0.9 Mpix	1920×1080 0.9–2 Mpix	1920×1080 0.9–2 Mpix	1920×1080 1–3Mpix (typically) Also 5+Mpix
Cables used for installation	Coaxial cable RG59 + power cable				LAN twisted pair cable-CAT5
	Maximum 100 m	Up to 500 m	500 m 300 m (1080p)	500 m 300 m (1080p)	Maximum 100 m
	LAN twisted pair cable Cat5 + Balun connectors. (Image quality is retained at a shorter distance compared to a coaxial cable)				PoE (data+power supply), or a separate power supply cable
Adjustment of cameras	Limited, directly at the camera (for most)	Directly at the camera via a joystick (for most)	Remote change of camera settings via a coaxial cable through DVR, including **through the Internet**	Remote change of camera settings via a coaxial cable through DVR	A particularly broad and convenient remote change of camera settings
Installation costs and installation complexity	A simple scheme, many wires	Simple installation	Simple installation, a single cable with several functions	Simple installation	The best opportunities for precisely adjusting the system for the specific requirements of each object
Other information		Relatively high quality, compatibility with lower quality cables and connections.			
			DVR supports analogue cameras and a limited number of IP cameras up to 2 Mpix	DVR supports analogue cameras and a limited number of IP cameras up to 2 Mpix	

[431] SIA Drošībai.lv (2018). Comparison of video surveillance systems. Retrieved from http://www.drosibai.lv/product/article/videonovroanas-sistmu-saldzinjums.html

The resolution could be one of the key aspects when choosing video surveillance cameras. The table shows that older model analogue cameras have a low resolution, while when comparing an analogue HD CVI and an IP camera, this difference is not that vivid. The resolution of both cameras is practically identical.

The next aspect addressed in the table is a comparison of the cables used and data transmission possibilities. The advantage of modern analogue cameras lies in the fact that it is possible to install them by using the existing coaxial cable, while there is also a limit to the maximum cable length if they are not used. HD CVI technology uses the same cables as the analogue system. The signal of analogue cameras can be transmitted also via the twisted pair cable Cat5, commonly known as a computer network cable. However, applying a purposely designed signal converter (Balun), one of the Cat5 pairs can be used for the transmission of an analogue signal. Additionally, a power supply can be connected to the remaining cable leads. As a result, one cable can be used for both: video and power transmission.

Adjustment of cameras. As seen in the table, in analogue systems it is possible to adjust only the analogue cameras themselves. Adjustment of settings of the modern analogue cameras can be performed through the coaxial cable and for HD CVI camera – through the internet, whereas the adjustment of IP cameras can be performed by the broadest of options, thanks to their connection with a computer network.

Installation. It is exactly the easiness of installation and the relatively low costs that make customers choose an analogue video surveillance system. It works under the condition that the surveillance object already has a video surveillance system installed and modern analogue systems are set up on the basis of the old cable network. However, if one needs to create a new system, it would be expedient to consider using an existing computer network or perhaps using a wireless video surveillance.

In conclusion, if you are looking for a new security system, you can go with different options. You can go the traditional analogue camera system route and have it be obsolete in a year or so. You can go with an HD-SDI (High Definition – Serial Digital Interface) camera system, which will give you some temporary benefits over HDCVI right now but will be obsolete in a few years. You can go with an IP megapixel system that will give you the ability to constantly upgrade over the years. Alternatively, you can go with an HDCVI system which has some minimal limitations on the resolution at the time being, but this is the technology that will wipe analogue and HD-SDI camera systems off the market.[432]

Assessing the video surveillance systems available on the market one can conclude that there are no clear parameters determining the superiority of one or another camera over the others. Modern analogue cameras will provide a relatively high quality, compatibility with lower class cables and connectors while offering limited possibilities for set-up adjustment. IP cameras will secure a high resolution, even beyond 5 Mpix, but this will also come at a higher price.

Therefore, the choice of a video surveillance system is determined by several aspects – costs, resolution as well as an opportunity to upgrade an existing video system and the prospects for further upgrades. Perhaps, due to the latter consideration, it is worth investing in the video system slightly more already today with a payback already in the nearest future. The rapid development of modern technologies requires investment, but it also offers unlimited possibilities.

[432] Security Camera King. (2016). The Differences Between HDCVI and Analog CCTV Security Camera Systems. Retrieved from https://www.securitycameraking.com/securityinfo/the-differences-between-hdcvi-and-analog-cctv-security-camera-systems

Conclusion

Looking at the contemporary video surveillance systems, their broad application and their impact on our daily lives, one must conclude that nowadays video surveillance equipment, as standalone units and part of a system, has become a secure method for ensuring the security of each individual and the overall security of companies, property and separate material values as well as ensuring the work discipline of employees.

The possibilities offered by video surveillance systems, individual equipment and software are being constantly perfected. These upgrades make video surveillance systems simpler, easier to use and allow to spend less time on the analysis of acquired data. They can provide high resolution, night vision, automatic recognition of car number plates, facial recognition, the remote guidance of cameras, multiple optical magnification, air and underwater surveillance, surveillance in places hard to access by people and many other functions highly useful for security.

Video surveillance has become an inevitable daily companion and an inalienable instrument of contemporary security and control. However, this reality requires a strong control over the surveillance processes and compliance with laws and legitimacy. Thus, the issue of privacy and lawful performance of video surveillance will always be topical. In order to protect the rights of citizens to privacy, some European countries have already introduced various limitations on surveillance, for instance, a ban on dashboard cameras.

References

Abramson, A. (2007). The History of Television 1942 to 2000. McFarland & Co Inc (Verlag), 319 p.

Caputo, A. C. (2014). Digital video surveillance and security. 2nd ed. Elsevier inc.

SIA Drošībai.lv (2018). Analogās AHD kameras un DVR. Retrieved from http://www.drosibai.lv/video-noverosana/ahd-kameras-un-dvr

SIA Drošībai.lv (2018). Explanation of video surveillance. Retrieved from http://www.drosibai.lv/video-noverosana/skaidrojumi-par-videonovroanu

SIA Drošībai.lv (2018). Comparison of video surveillance systems. Retrieved from http://www.drosibai.lv/product/article/videonovroanas-sistmu-saldzinjums.html

SIA EMEM (2007). Video Surveillance Resolution CIF/D1/960H/720p/1080p Difference and Comparison with Different Standards. Retrieved from http://www.vns.lv/index.php?aux_page=aux24

HD Analog.com (2015). AHD CCTV Technology Commonly referred to as: AHD, Analog HD. Retrieved from http://www.hdanalog.com/options/ahd.html

Shenzhen MVTEAM Technology Co., Ltd. (2018). What's the relative merits of transmission modes (POE,EoC,PLC) for CCTV System? Retrieved from https://www.mvteamcctv.com/news/What-s-the-relative-merits-of-transmission-modes-POE-EoC-PLC-for-CCTV-System.html

TechTarget (2010). IP camera. Retrieved from https://whatis.techtarget.com/definition/IP-camera

Security Camera King (2016). The Differences Between HDCVI and Analog CCTV Security Camera Systems. Retrieved from https://www.securitycameraking.com/securityinfo/the-differences-between-hdcvi-and-analog-cctv-security-camera-systems

About the Authors

Vilnis Veinbergs, *MPA*
Bachelor degree in Personnel Management Psychology and Master degree in Public Relations. Currently a doctoral student in Business Administration study program at the Turiba University.
Retired officer, Major of the National Armed Forces of the Republic of Latvia. Worked in the Security Service of the Republic of Latvia as a specialist of the personal security of the country's highest officials. Currently Head of the Internal Security Service and Director of Organisation and Individual Security study program at the Turiba University.

Dainis Siliņš, Student of Turiba University professional bachelor study program "Organization security"

FIRE SAFETY SYSTEMS

Uģis Začs
Viktorija Ratačova

Introduction

The selected theme is highly topical since fire safety is one of the key security risks, which should be paid close attention already during the design phase of a facility. The main fire safety feature deserving careful attention is a timely detection of fire or fire threats and notification of people about the start of an emergency situation, in this case – fire. Automatic fire detection and alarm system is particularly important in the cases when a dangerous situation is formed in a building visited by a large number of people and the visitors need to be notified of the threat. Malfunction of the system or its improper installation and service can lead to a grave tragedy, experienced by the Russian city of Kemerovo on 25.03.2018.

The objective of the work is to analyse various types of fire safety systems and to summarise information on their effectiveness.

This chapter explains the importance of these systems and actions to be taken as well as deals with additional aspects affecting fire safety at various facilities.

Each country has its own binding normative acts regulating both – installation and service of the system. If construction of new facilities is planned, the parties engaged should envisage all the necessary measures for the implementation of the norms already at the design and development stage. There are also common European Union standards, which must be observed, and which are used as the basis for developing national normative acts of individual EU member states. In addition, the existence of automatic fire safety systems is one of the key points when arguing about lower insurance premiums.

When reviewing the totality of a fire safety system, it can be divided into three large groups:

1) automatic fire detection systems;
2) automatic fire voice notification systems;
3) automatic fire extinguishing systems.

According to its structure, an automatic fire detection and alarm system is one of the most complicated safety systems and, therefore, its installation must be performed at a high-quality level. An in-depth understanding and design and development of fire safety systems require engineering and technical knowledge and education. According to the author, nowadays many people working in the field of safety lack general knowledge and understanding on the principles and application of fire safety system operation. Therefore, it is important to educate people, particularly those employed in the field of security.

1. Automatic fire detection systems

Automatic fire detection system or a fire alarm. Two types of fire alarms are normally being utilised:

1) **conventional (analogue)** fire alarm system;
2) **addressable** fire alarm system.

It is recommended to install a conventional (analogue) fire safety alarm system in small facilities where a small number of fire safety detectors is sufficient. A conventional (analogue) fire safety alarm is installed by dividing fire safety alarm detectors according to zones or loops, which, in case of fire, allow the fire safety alarm system's control panel to identify the zone or loop with a larger number of detectors (for instance: ground floor with 4 detectors).

It is recommended to install the **addressable fire alarm** system at facilities requiring a large number of fire alarm detectors or when it is important that the facility upholds an increased level of security with a rapid reaction capability. Within the addressable fire safety alarm system each fire safety alarm detector has a designated address and each detector is easily identifiable (for instance, detector 001 – ground floor, room 1). In case of fire or damage, this system provides the alarm control panel with a capacity to identify precisely the location of fire or damage. Addressable fire safety alarm systems are increasingly equipped by supporting visualisation. Visualisation means that the facility plan with the specific triggered area is reflected on a computer screen providing easier orientation for the staff on duty.

An automatic fire detection system must be serviced regularly and the service intervals should be selected according to the technical regulation requirements of the producer, national fire safety regulations and the binding European standards.

These systems are normally installed in the duty staff room on the ground floor of the building, but in cases if the facility does not employ a twenty-four-hour duty staff, the system can be set up in a way that it sends a signal to the main switchboards of cooperation partners.

The automatic fire detection system includes:

1) **control panel** – or a control unit which reflects the operation of the fire safety alarm system, including triggered alarms, damage and activities performed. The control panel provides for viewing of event history, for

accepting alarm, for launching a fire safety signal, for isolating detectors or zones, etc.;

2) **detectors** – the fire safety system uses several types of detectors:

Picture 1. **Optical smoke detector of the fire alarm**[433]

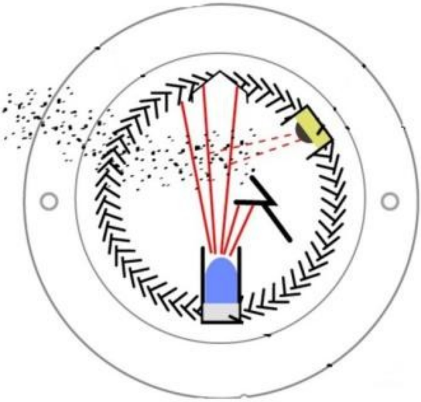
Optical fire detector is activated by:

1) dust;
2) vapours;
3) smoke.

When the detector has been activated, its red indicator light turns on.

Optical fire detector is triggered by an activated photo-diode sensor (Picture 2).

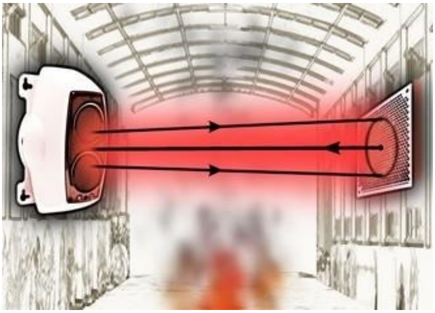
[433] Unpublished materials of SIA GRIFS AG



Picture 2. **The optical photo-diode sensor has been covered by dust**[434]

Heat detector. The heat or temperature detector of the fire safety alarm is activated by the impact of a rising temperature. The detector activation temperature should be set depending on the place of its use. When the detector has been activated, its red indicator light turns on.

Smoke beam detector (Picture 3):



Picture 3. **Smoke beam detector of the fire alarm**[435]

[434] Unpublished materials of SIA GRIFS AG

[435] Ibid

The smoke beam detector of the fire alarm consists of a transmitter and a reflector. The transmitter of the smoke beam detector transmits a beam against the reflector and receives the already reflected beam, and, as soon as smoke appears, the beam is reflected as broken resulting in detector activation. In case when the transmitter is out of position or the beam shifts and the transmitter does not see the reflected beam, its shows a malfunction.

It is important to be aware of the detectors and the principles of their operation not only at the time of their installation and service but also the time of any reconstruction, repair works or other activities at the facility, which can create dust or activate the system by any other means.

Thermal cable – a special cable, which connects parts of the system (depending on the specific character of the protected rooms or equipment).

Manual alarm button (Picture 4) – is designed for cases when a person notices a fire hazard threat before the automatic system has been triggered and notifies of the fire threat manually.

Picture 4. **Manual alarm button of the fire detection system**[436]

[436] FL_MCP_MMF301_datasheet. (2018). System product enterprises (I) PVT. LTD. Obtained from http://www.speipl.com/index/products_inquiry/25/4/Mineral_Insulated_Copper_Cabel

Alarm sirens (Picture 5) – designed for informing people of the fire threat locally. Alarm sirens are installed as a separate system, which is combinable with the automatic fire voice notification system. The fire alarm siren sounds at a highly piercing pitch and is a harbinger for evacuation.

Picture 5. **Manual alarm button of the fire detection system**[437]

The automatic fire detection system is highly important because it excludes a possibility of a human error. For instance, while people fall asleep at night and do not feel or see the moment of the start of the fire, the system does not sleep, it activates automatically and issues an alarm in order to mobilise guards and staff on duty. Another important aspect to remember is the fact that in order to detect the start of the fire in a timely way, the system detectors can be placed even at the most complicated locations, for instance, at suspended ceilings, which often house various communications, lighting installations or other technical systems, which can cause fire.

[437] Siren 100dB, addresses IP52 ESI-50 Esmi (2018). SLO Latvija. Acquired from https://www.slo.lv/lv/veikals/produkts/?id=62122

2. Automatic fire voice notification systems

A voice notification system (Picture 6) is a totality of equipment which ensures provision of various types of information to visitors of the facility and is also referred to as a public address system. This system is used on a daily basis for providing operational information on forgotten or misplaced items, incorrectly parked cars, for transmitting advertisement jingles, etc. The system is highly important in emergency situations as it is a means of informing visitors on the emergency situation. The system can be activated manually, by triggering a particular algorithm, and the system can be programmed for automatic activation (for instance, after activation of two fire safety detectors next to each other). The system can be used in order to produce verbal announcements on the safety situation at the facility. The voice notification system is programmed in the way that its manual activation or automatic activation for emergency notification turns off all other sound and music leaving it on only for the purpose of an announcement. When setting up an automatic voice notification it is recommended to make sure that the information is provided in the state language as well as in an international (English) language.

In the case of Latvia, the automatic notification is performed in Latvian, Russian and English. Information announced must be as brief, concise as possible and it must contain directions on what the visitors of the facility must do.

Picture 6. **Voice notification system**[438]

The voice notification system consists of a control unit, an amplifier, loudspeakers located in the rooms of the facility and at its perimeter, microphones and cables. It is recommended to divide the system into several zones depending on the size of the facility (for instance, auxiliary premises and public areas).

3. Automatic fire extinguishing systems

An automatic fire extinguishing system is built during the construction of a facility and in compliance with the normative acts enforced at the time of construction. An automatic fire extinguishing system is mostly understood as a sprinkler system. Water is the most accessible substance with good cooling qualities and, therefore, is most commonly selected for an automatic fire extinguishing system for the fire protection of premises and buildings. Moreover, water-based fire extinguishing systems are the easiest to design and mount. Water-based fire extinguishing systems can be either sprinkler or drencher systems.

[438] Notification and background music system (2018). Telekom serviss http://www.ts.lv/lv/services/security-systems/public-address/

Sprinkler fire extinguishing systems (Picture 7):

Picture 7. **Automatic fire extinguishing systems – sprinklers**[439]

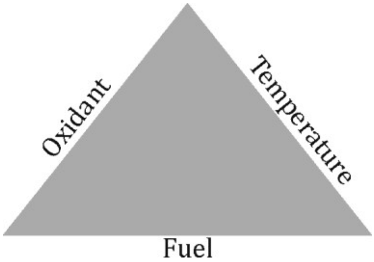
Sprinkler fire extinguishing systems have built-in sprinklers (drizzlers or dispensers). Tubes of an automatic sprinkler fire extinguishing systems constantly contain either pressurised water or, in cases when a tube is located in a place subjected to fluctuations of temperature (e.g., a multi-storey open-air parking lot) – pressurised air.

Sprinklers are activated as a result of changes of pressure in the system. In case of a fire, the room temperature rises and when reaching a certain threshold it bursts the thermo-sensitive element located inside of a sprinkler. The thermo-sensitive element itself houses a capsule containing an alcohol-based liquid. After the thermo-sensitive element bursts, water starts to pour from the sprinkler. The construction and the principles of operation of an automatic drencher fire extinguishing system are very similar to the sprinkler fire extinguishing system, but the drencher system does not contain a thermo-sensitive element. The drencher system constantly stands in an open mode. The difference between the

[439] Sprinklers (2018). FM Approvals. Obtained from https://www.fmapprovals.com/products-we-certify/products-we-certify/sprinklers

drencher and the sprinkler automatic fire extinguishing systems lies in the fact that, in a case of a fire, sprinklers provide spraying of water only above the fire – at the location of a rising temperature, which has burst the thermo-sensitive element, while drenchers spray water across the whole pre-programmed area. The sprinkler system can be activated accidentally by damaging the thermo sensitive element, for instance by washing ceiling with a broom and breaking the capsule. Both systems are effective and do not threaten human lives. The water extinguishing system requires additional elements like a pumping station providing the required water pressure. Pressure is mostly provided by water pumps. It is recommended to equip a facility with two different types of pumps. One of them could be an electrical pump for the occasions when the facility has not lost power supply, while the other could be a fuel driven pump for the occasions when the electric power supply has been lost.

Besides the automatic water extinguishing systems, there are also powder-based fire extinguishing systems. Powder-based fire extinguishing systems use powder as an effective firefighting means. Powder is used in those facilities which must not be subjected to water. The advantages of the automatic powder-based fire extinguishing system lie in its relatively low costs, easy installation and a possibility to move this system from one room to another upon necessity. As opposed to the automatic gas or aerosol fire extinguishing systems, rooms with a powder system do not need to be leak-proofed. In case of a fire, rooms equipped with a powder-based extinguishing system do not require to be disconnected from electrical power supply. Compared to the water extinguishing systems, there are smaller losses resulting from fire extinguishing operation, the powder stays inside the particular room, while water will flow down to the very bottom of a building. In facilities equipped with automatic water fire extinguishing systems, it is recommended to place all household items (equipment, goods, belongings, etc.) on an at least 10 cm high elevated surface. The types of powder differ depending on their application and it is recommended to choose them individually, depending on the type of a protected facility and valuables located there. The impact of powder is based on extinguishing of the burning element and dispersing of powder across the burning surface thus creating obstacles and encumbering the burning process. As opposed to the automatic water extinguishing system, the powder-based system can be harmful to human life and health and, therefore, it can only be applied upon condition that people are not present in the particular area or people have been evacuated. In most of the cases, this system is programmed for manual activation during the periods when people are expected to be present and for automatic activation when they are expected to be away. Besides the powder extinguishing systems, there are also gas based fire extinguishing systems. Nowadays, it is exactly the gas-based extinguishing systems that are used broadly and effectively. In case of a conflagration or upon detecting fire, the extinguishing system evolves gas, which decreases the concentration of oxygen in the room resulting in the elimination of fire. A fire can be in place if the following three preconditions are fulfilled – there must be something that burns (an item, fuel, a body, part of a building, etc.), there must be oxygen and there must be a particular temperature which causes ignition of a particular item (Picture 8). If one of those factors is excluded, the fire dies out.



Picture 8. **A fire triangle**[440]

Similarly to the powder extinguishing system, the gas-based extinguishing system can also be harmful to human life and health and therefore it can only be applied upon a condition that people are not present in the particular area or people have been evacuated. In most of the cases, this system is programmed for manual activation during the periods when people are expected to be present and for automatic activation when they are expected to be away. As opposed to the powder extinguishing system, this system requires a leak-proof room preventing the outflow of gas and the inflow of oxygen, which enhances the process of burning.

All fire safety systems at a facility are built as a single large system in order to make them operate as a large unified body.

Additional opportunities for fire alarm and management of the technological processes of a facility:

1) blocking/opening of doors upon activation of a fire safety system;
2) blocking and opening of elevators and escalators. In order to establish the fact that the elevators are empty and to make sure that people do not use them in case of a fire, elevators should go down automatically and open on the

[440] Unpublished materials of SIA GRIFS AG

ground floor. Elevators are the largest chimneys of a building;

3) switching off of the ventilation system – for the purpose of decreasing the inflow of oxygen and limiting the spread of fire;
4) opening of smoke discharge hatches/windows – for the purpose of elimination of smoke and providing an easier view on fire sources which should be put out;
5) blocking/launching of various technical devices;
6) sending of the fire safety system signal to the switchboard of cooperation partners in order to even out the risks if the staff on duty has not registered the activation of the system;
7) connecting of the automatic fire extinguishing system with the BMS (building management system) management system;
8) placement of smoke curtains at a facility in order to separate zones and to prevent fire from spreading rapidly from one room to another.

Fire safety systems will not be effective if the facility does not have well-developed actual procedures, instructions and course of action in case of a fire or emergency instructions describing step-by-step actions of what actions have to be performed and what is ensured by the systems in place.

Conclusions and suggestions

Fire safety systems are diverse and complicated systems whose installation, presence and service are regulated by normative acts of each country. In compliance with the normative acts, facilities are equipped with modern fire safety systems, which the staff on duty is not capable to deal with in full. There is a wide variety of fire safety systems, which together form a single large system capable of operating both autonomously and manually with the engagement of the staff on duty.

Based on the conclusions, for the purpose of fulfilling duties in a professional way, it is important that each member of the guarding staff, people employed by security structures or staff on duty of a facility know the basic principles of fire safety system operation. To define in one or another normative act that each facility must contain an easily accessible and comprehensible scheme outlining how to deal with a particular fire safety system thus making it easily understandable to outsiders. In order to decrease a possibility for a human error, when creating systems one should think of the most effective way of making those systems operate autonomously without the engagement of staff of duty.

References

FL_MCP_MMF301_datasheet (2018). System product enterprises (I) PVT. LTD. Acquired from http://www.speipl.com/index/products_inquiry/25/4/Mineral_Insulated_Copper_Cabel

Siren 100dB, addresses IP52 ESI-50 Esmi (2018). SLO Latvija. Acquired from https://www.slo.lv/lv/veikals/produkts/?id=62122

Notification and background music system (2018). Telekom serviss http://www.ts.lv/lv/services/security-systems/public-address/

Sprinklers (2018). FM Approvals. Obtained from https://www.fmapprovals.com/products-we-certify/products-we-certify/sprinklers

Unpublished materials of SIA GRIFS AG

About the Authors

Uģis Začs, MBA
Uģis Začs received a Master's Degree in Business administration at the Riga Business School in 2015 and Bachelor's Degree in Regional development and governance at the Latvian University of Agriculture in 2011.
The author works in one of the largest security companies in Baltic States – SIA GRIFS AG – since 2006. The author works as a corporate client security manager and in his daily life deals with physical and technical security, manages different kind of objects, develops security concepts, and controls the security status of facilities. The author is also a lecturer at the Turiba University, the programme on Company Security.

Viktorija Ratačova, student of Turiba University professional bachelor study program "Organization security".

ACCESS CONTROL SYSTEM

Uģis Začs

Introduction

The selected work theme is topical since the security of each organisation and each facility starts with an introduction of either a correct or an erroneous access control system. There are many different types of facilities and each facility has a stronger or less stringent access control regardless if it is an ordinary key or complex biometric solutions. Each company or facility can choose an optimum solution targeted at making its facility or a totality of facilities more secure. For the purpose of diminishing human impact on access control procedures people increasingly choose technical solutions.

The objective of the chapter is to research access control systems by starting with the simplest and to provide their description in a structured manner on the basis of their functionality.

1. Access control systems and their types

A correct and thought-out procedure of access to a facility and movement inside of it is one of the integral parts of the development of a security concept for a facility. Nowadays, there are various technical solutions and systems available targeted at decreasing an opportunity for human error and the engagement of people in controlling this procedure. In this chapter the author reviews and describes several technical solutions, which help and ensure a controlled access to a facility. The author provides an overview of both – simple solutions and more complex multifunctional systems. This chapter deals with issues of how to approach access control systems, how to choose the most economically viable solution for gaining maximum effectiveness from the system selected. In addition, the functions and gains from the contemporary access control system are also provided.

As opposed to the compliance requirements related to the installation scope, selection being strictly defined in the normative acts of each country regarding fire safety systems, the choice of access control systems primarily remains the choice of each separate facility itself. Choosing the best, the most effective and economically viable way of providing access control at a facility poses the biggest challenge for a security expert. In order to gain a better understanding of the system and for the purposes of choosing the right system, one must define the goal of introducing such an access system in the first place. The choice of an access system is closely linked with the development of a security concept for a facility, since it regulates the movement of people and restrictions on it. For the purposes of reviewing access control systems, they can be divided into two large groups:

1) a single delimitation system (doors, gates, fences, etc.): opening/closing;
2) a multi-delimitation system (doors, gates, fences, etc.): opening/closing.

One aspect of choosing the right access control system is related to the importance of providing the required access and control. However, there is another issue of how this system will function in a crisis situation, particularly if the facility hosts many people, and how this system will affect evacuation.

If it is necessary to create access control for a single delimitation, there are several options.

A key – one key, which unlocks a specific delimitation point, is the most common type of access control used by households as well as at various facilities. When choosing a key it is important to select a trustworthy key producer. Keys have several levels of security. In addition to the selection of a key system, the selection of doors and locks is also highly important. One should assess risk factors related to break-ins, fire hazard, etc. For instance, by choosing metallic doors one should keep in mind that metal expands when subjected to heat and it will not be possible to open them in case of fire. The use of a common key is an effective way of restricting access if the key is used by one person only. If the same key is used by several persons there is a risk that the key will be copied. If each room of a facility has its own key, locking a particular door, a key circulation system should be created. During the development of a system, one should envisage registration of keys and making sure that the keys are not removed from the facility. The lack of registration of opening a delimitation point and the lack of identification of a person opening it represents a drawback of using keys. In order to ensure its registration, one should install additional security systems, for instance, video surveillance. It is important to perform a regular audit of keys in order to make sure that all keys are in place and have not been lost. If a key is lost, the lock on the particular door should be replaced. When evacuating a large facility with many rooms and delimitations one has to carry a large bundle of keys.

Mechanical keypad lock (Picture 1) – a mechanical lock installed on a particular point of delimitation opening a single delimitation. These types of locks are most commonly used at the entrance doors of blocks of flats or at less significant rooms and places, for instance, at the doors of garbage disposal storage rooms. The delimitation point opens after a particular combination of buttons have been pressed on the mechanical keypad lock. There is a risk of providing unregistered access rights to other persons, as well as a risk related to abrasion affecting those keys, which are used all the time, thus making it possible for an outsider to guess the right combination. Therefore, it is important to clean the lock itself in order to make sure that the abrasion marks are not visible. The positive aspect of using this lock lies in the fact that it is not necessary to carry around a key, as it can be easily lost. It is important to change the code regularly in order to control the number of people who have access to a particular area.[441]

Picture 1. **Mechanical code lock**[442]

[441] Unpublished materials of SIA GRIFS AG

[442] Smart Keypad Door Lock Password Lock Mechanical Key Locks for 45–55 mm Thickness Door Silver (2018). aleksnld.com. Acquired from https://alexnld.com/product/smart-keypad-door-lock-password-lock-mechanical-key-locks-for-45mm-55mm-thickness-door-silver/

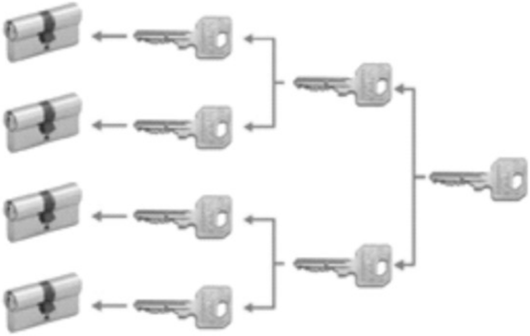
Electronic code lock (Picture 2) – a device similar to the mechanical code lock, but with several improvements. The input of a code takes place by pressing keys on the keypad one by one. Therefore, even if the keys have suffered from abrasion, it is much more difficult to guess the access code, due to its many possible variations. In addition to the code, the lock can also be opened with a unique chip, the size of a small pendant. Losing the chip constitutes an additional risk. The devices of this type are often linked with door intercoms and it is possible to contact a person inside a facility. One can often come across a situation when a company which has installed the lock has provided an identical code to a whole range of its locks.

Picture 2. **Electronic code lock**[443]

If it is necessary to create access control for several points of delimitation, there are the following options.

[443] Unpublished materials of SIA GRIFS AG

Multi-level lock system (Picture 3) – one of the most commonly used access control systems. The essence of the system lies in divided access opportunities based on keys. There are several levels of keys, where the lowest level can unlock only a particular door, a higher level can unlock groups of doors and the highest level or the "master key" unlocks all doors. Similarly to ordinary keys, it is important to establish a key circulation procedure and to control carefully the higher level keys, since losing a master key results in the necessity to re-programme all keys, and this procedure is expensive. This system is normally used together with some other access control systems. The biggest advantage of this system lies in the fact that one key is sufficient for opening, for instance, 100 different delimitation points and no large key bundles are needed. However, also under this system, it is not possible to identify when and who has unlocked a certain delimitation point unless another security system is also employed.



Picture 3. **Reflection of the operation of a multi-level lock system**[444]

[444] Master Key door lock systems (2018). ASSAZ. Acquired from http://www.assaz.lv/master-key-sistemas-izstrade

Proximity access card (Picture 4) – one of the most common access control systems. In order to introduce proximity access cards at a facility, one should take into consideration that it will demand greater investment. Successful functioning of the system requires a dedicated computer, which is connected to the overall access control system, there is also a need for specialised card readers, connected to the overall system and separately – to a particular delimitation point. In addition, the system requires a specialised computer software, which administrates various access levels and cards. Separate cards must also be purchased for each employee.

Picture 4. **Proximity access card**[445]

Depending on the software installed, this access control system offers a broad range of possibilities:

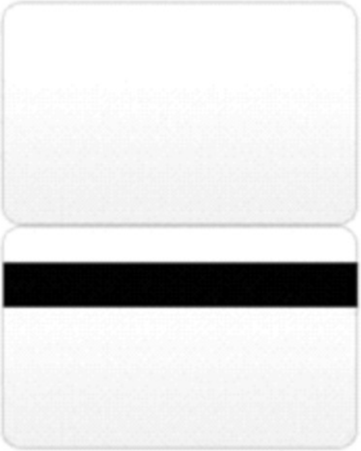
1) to identify a particular person who has used the card, the time and place of access;
2) to follow the complete route of a person, identifying the time and place of movement;

[445] Proximity Access Card Rs 15 (2018). Indiamart. Acquired from https://www.indiamart.com/proddetail/proximity-access-card-13289664748.html

3) to identify precisely the access to rooms and places of each person holding an access card;
4) to set access timing, i.e. a card can be programmed to open a particular delimitation point during a particular period of time;
5) access rights and restricts are easy to be set up;
6) information on card usage is stored for a long period;
7) the system reflects the number of people in the facility and, in case of evacuation, it provides exit information on how many people were or still are at the facility;
8) the system can be used as an employee time-sheet system by introducing a procedure when an employee signs in with his/her card upon arrival and signs out upon departure;
9) the card can be granted an additional function by integrating it with the guard alarm system: when opening a delimitation point, the proximity access card can also switch off the alarm of a particular room;
10) the card operates also through a cover and thus can be carried in a wallet;
11) the cards can also be personalised by printing on information regarding a particular person, e.g. a photo, which can assist in the control function and preclude people from passing cards to the third parties.

The system can be used both – inside and outdoors. Due to the fact the card does not have to touch the reader and it operates from 5 to 30 cm from the reader, both – cards and readers have a long service lifetime. This system also requires the establishment of a specialised procedure regulating what type of access should be provided to particular people, the procedure of notification if a card is lost and its cancellation or to avert that access is still accidentally provided to persons who no longer work at the facility.

Magnetic card (Picture 5) – a magnetic card offers possibilities, which are similar to the ones of a proximity access card. All of this depends on the type of computer software installed. The difference between the two cards lies in the fact that the proximity access card contains a microchip while the magnetic card operates on the basis of a magnetic strip. The magnetic card must be swiped along a specially designed reader, which constitutes a drawback since every swipe contributes to its wear.



Picture 5. **Magnetic access card**[446]

Car plate readers – car plate recognition systems are becoming increasingly popular for the purposes of traffic control.

[446] Manager POS Access Card (Magnetic:MSR) (2018). Next Kernel Inc. Acquired from https://www.nextkernel.com/shop/product_info.php?products_id=117

The system includes an IP surveillance camera, a work computer and a specialised computer software. The possibilities offered by the system depend on the software applied. The advantage of the system lies in the fact that it operates on a 24-hour basis and with unchanged capacity, while a person is capable of letting a car slip by or of missing a car which has arrived. Access to particular cars with particular national number plates is granted by means of input of information and configuration of the specialised software. It is also possible to set access timing. Upon arrival at the gate or at the barrier, the car stops and at that moment the software utilises a video surveillance camera, reads the car plate number and either lets the car in or denies access. The software has some imperfections, for instance, if part of the number plate is covered by snow or dirt, the software may not recognise the number. It is also possible to utilise fake number plates of a car, which is known to have an access to the particular facility.

Biometrics: the totality of physical features and indicators of a physical person [facial digital image, traces of fingers (palms) or prints].[447]

Fingerprint scanner (Picture 6) – various biometric data readers become increasingly accessible and more popular. The principles of operation are similar to the operation of proximity and magnetic access systems with the difference being that the card is replaced with human biometric data. The advantages of the system lie in that fact that it does not require additional expenses on specialised cards and biometric data is hard to lose. The disadvantage of this system could be seen on occasions when a person, for

[447] The Law on Biometric Data Processing. Adopted on 21.05.2009. *Latvijas Vēstnesis*, No. 90 (4076), 10.06.2009., *Ziņotājs*, No. 13, 09.07.2009. Latest amendments 05.07.2017, Article 1

instance, injures his/her finger, the print of which is used for biometric data purposes. Such a situation may result in the system refusing to recognise the print and will not open the barrier. Fingerprints are the most commonly used biometric data.

Picture 6. **Fingerprint scanner**[448]

Retinal scanning – one of the types of biometric reading, which is not that popular and is not considered convenient.

Overall, there are various technical solutions, which assist in organising and controlling access of people to facilities. In case of a necessity to impose stricter and more secure requirements on the access of people to a particular facility are necessary, it is recommended to apply more than one system by forming a combined access control system. For instance, a code and fingerprint scanning represents a combined type of access control. An access control system is often combined with a guarding system, thus achieving interaction between the two systems resulting in a higher security of a facility.

[448] Fingerprint Scanner Door Access System (2018). HTCcomunity. Acquired from http://htccommunity.org/fingerprint-scanner-door-access-system-D147464/

Another system, which indirectly assists in controlling access to a facility is an alarm system, particularly door magnets, Guard alarm systems can precisely identify opening of one or another door of a facility. It is also possible to programme doors in a way that the system will notify if any doors stay open longer than a predefined period of time, allowing guards to check its cause.

Tourniquet (Picture 7) – one of the delimitation devices, which can be used in the access control of persons. The main advantage of a tourniquet is its capability to provide access of people to a facility one by one (unless it is a bigger tourniquet designed for two persons). The main risk associated with a tourniquet is related to evacuation – in case of an evacuation, a tourniquet would encumber exit from a facility. Therefore, it is necessary to envisage a system or a procedure for turning it off in such cases.

Picture 7. **Tourniquet**[449]

[449] Tourniquet (2018). AVIX. Acquired from https://turnikets.ru/

Hydraulic road blockers (Picture 8) are designed to protect drive-in territories from unwanted vehicles.

Picture 8. **Hydraulic road blockers**[450]

Such barriers are installed in public areas – places gathering large numbers of people, therefore decreasing the risk of a car hitting the crowd. Hydraulic road blockers can also protect facilities from being hit by a car – show-windows or interiors of buildings.

Conclusions and suggestions

Security experts and persons in charge of security of facilities do not have enough understanding of how to select the most effective access control system. Most of the facilities do not have even a minimum of predefined requirements regarding access control systems. In many places, access control systems are not used at their full capacity. In cases when there is an absence of internal regulations of facilities, which describe access procedures, access control systems are not effective.

[450] Painted steel hydraulic security road blockers at an increased street traffic capacity, with LED light. (2018). GS Total Security solution. Acquired from http://lv.xraysecurityscreening.com/automatic-bollards/automatic-rising-bollards/stainless-steel-hydraulic-automatic-rising-tra.html

Based on the conclusions, security experts or persons in charge of security must learn the types of actions and the basic principles of access control systems or they must engage industry experts in order to gain the capacity of assessing and developing a concept and procedure of accessing a facility. There is a need to regulate and define the requirements in one of the normative acts, which must be observed when constructing a new facility and developing its access control system. For the purpose of an effective use of a selected system and its functioning according to its designed purpose, before choosing an access control system one must carefully assess all the risks, which can endanger a particular facility and clarify all the possibilities and advantages offered by one or another security system (access control system). Each facility with an access control system requires that it operates on the basis of developed internal procedural regulations, that there is a clearly defined access procedure in place and that this procedure is being controlled.

References

The Law on Biometric Data Processing. Adopted on 21.05.2009. *Latvijas Vēstnesis*, No. 90 (4076), 10.06.2009., *Ziņotājs*, 13, 09.07.2009. Latest amendments 05.07.2017.

Painted steel hydraulic security road blockers at an increased street traffic capacity, with LED light (2018). GS Total Security solution. Acquired from http://lv.xraysecurityscreening.com/automatic-bollards/automatic-rising-bollards/stainless-steel-hydraulic-automatic-rising-tra.html

Fingerprint Scanner Door Access System (2018). HTCcomunity. Acquired from http://htccommunity.org/fingerprint-scanner-door-access-system-D147464/

Master Key door locking systems (2018). ASSAZ. Acquired from http://www.assaz.lv/master-key-sistemas-izstrade

Manager POS Access Card (Magnetic: MSR) (2018). Next Kernel Inc. Acquired from https://www.nextkernel.com/shop/product_info.php?products_id=117

Proximity Access Card Rs 15. (2018). Indiamart. Acquired from https://www.indiamart.com/proddetail/proximity-access-card-13289664748.html

Smart Keypad Door Lock Password Lock Mechanical Key Locks for 45mm-55mm Thickness Door Silver (2018). aleksnld.com. Acquired from https://alexnld.com/product/smart-keypad-door-lock-password-lock-mechanical-key-locks-for-45mm-55mm-thickness-door-silver/

Tourniquet (2018). AVIX. Acquired from https://turnikets.ru/

Unpublished materials of SIA GRIFS AG

About the Author

Uģis Začs, *MBA*

Uģis Začs received a Master’s Degree in Business administration at the Riga Business School in 2015 and Bachelor's Degree in Regional development and governance at the Latvian University of Agriculture in 2011.

The author works in one of the largest security company in Baltic States – SIA GRIFS AG – since 2006. The author works as a corporate client security manager and in his daily life deals with physical and technical security, manages different kinds of objects, develops security concepts, and controls the security status of facilities. The author is also a lecturer at the Turība University, the programme on Company Security.

SECURITY GUARD MANAGEMENT CENTRE

Uģis Začs
Dzintars Rendenieks

Introduction

The selected theme is topical, since the organisation of security of a facility, the choice of a commercial agent, which would provide security guard services or the construction of a security guard management centre/control room requires a clear understanding that the centre is or will be protected against various risks, for instance, against the loss of electrical power, an armed attack, etc. Security guard centres mostly hold a lot of different information on various clients and on security concepts of various facilities. Therefore, it is important that this information is secured to a maximum and is protected against access by the third parties.

The objective is to research the means of protecting a security guard management centre/control room against the existing risks.

1. Management centre/control room

Management centres/control rooms do not exist solely in the area of security guard activities. National security structures, State police, municipal police and others have their own management centres/control rooms. Their existence, requirements and operations are strictly regulated by the existing normative acts of the country. The author believes that the acceptance of inadequately created and equipped management centres/control rooms is the biggest mistake that commercial security guard providers, internal security services and other security structures often make. The author reviews the requirements on security management centres/control rooms established in the normative acts. Reviewing security guard management centres, the main normative acts regulating this area in Latvia is the Cabinet of Ministers Regulations No. 757 (09.12.2014). These regulations define the requirements regarding security guard management centres and they can be divided into separate groups.

1.1. Room set-up and functionality

1. A security guard management centre is set-up in the real estate property rooms, which are owned, possessed or held by the respective commercial agent.
2. In compliance with the construction standard of Latvia, which establishes the fire safety requirements, a security guard management centre must be set up in a V usage type of building, which is at least U2-level fireproof.
3. The minimum totality of connected rooms of a security guard management centre is a room with a monitoring and alarm signal reception switchboard (hereinafter – the main switchboard) installed, an antechamber for controlling the entry of persons in the main switchboard room, and auxiliary premises (a toilet, a recreation area, a fuel generator room).
4. The exterior walls and the interior walls separating it from other premises of the building are made of a 200 mm massive brick wall or at least of 150 mm molten core-concrete or at least 100 mm reinforced concrete. The ceiling and floors are made of 150 mm molten core-concrete or at least 100 mm reinforced concrete.

5. Entrance doors of the security guard management centre are made of metal with a 45 mm or thicker door leaf and the thickness of metal plates of the door must be at least 2 mm; doors must be locked with a multi-point lock and equipped with a cylinder-shaped bolt and a tightening mechanism.
6. The entrance of the security guard management centre is equipped with an intercom and an access control device.
7. Windows of the security guard management centre are covered with a coating, which prevents seeing the inside of the room from the outside and the security class of window glassing must not be lower than EN1063 BR3NS.[451]

This group of demands strictly regulates the technical requirements of the room and its construction, which must be observed in order to guarantee the minimum security level at the security guard management centre/control room and ensures that these requirements serve as an implementation standard for those companies, which provide technical guarding services.

1.2. The setup of the room to prevent emergency and in the case of emergency

1. The building, which houses a security guard management centre has an evacuation exit.
2. The room of security guard management centre/control room is equipped with heating, ventilation and climate control systems.
3. The building, which houses a security guard management centre/ control room is equipped with a lightning protection system and

[451] Regulations of the Cabinet of Ministers No. 757. Regulations on the licensing of security guard activities. Adopted on 09.12.2014 Published: Latvijas Vēstnesis 257 (5317), 30.12.2014 Article 2

ground bed contours in compliance with the construction standard of Latvia establishing construction of internal electrical installations of buildings.

4. A security guard management centre is equipped with a fire detection and an alarm system.
5. Upon receiving a signal from the technical guarding system installed at the protected facility, the main switchboard transmits a visual and a sound signal as well as stores information on the activation of the technical guarding system and provides an opportunity to view and print out this information.[452]

However paradoxically it may sound, but guarding commercial agents, who are engaged in providing security to their clients, often forget about their own security and the security of their management centre. Therefore, it is important to create as secure and comfortable conditions to employees working there as possible without forgetting about fire safety on the premises. Premises of this type, which is a place of active work and which houses lots of different security systems, are subjected to a high level of fire threat. This is caused by the presence of various technical systems operated on a 24/7 basis, which may fail due to their heavy workload and may cause fire.

1.3. Ensuring of uninterrupted operation

1. A security guard management centre is provided with an uninterrupted electrical power supply by using a permanent electrical connection with sufficient power and a backup electrical supply –

[452] Regulations of the Cabinet of Ministers No. 757. Regulations on the licensing of security guard activities. Adopted on 09.12.2014. *Latvijas Vēstnesis,* No. 257 (5317), 30.12.2014, Article 2

UPS (uninterrupted power supply) and a fuel power generator of a sufficient capacity.

2. In case of a voltage breakdown, the backup fuel power generator turns on automatically, providing an uninterrupted operation of the main switchboard and the related monitoring, data storage, communication, alarm functions and the operation of other equipment and systems of the centre until the permanent electrical supply is restored.
3. The reserves of the local fuel power generator ensures its operation for 24 hours.
4. UPS and the fuel power generator are located separately, in a room equipped with security guard and fire protection systems and secured against an unauthorised access.
5. Electrical wires and cables located outside the premises of the security guard management centre/control room are secured against physical and fire damage.[453]

It is highly important that a place with so many technical systems involving information processing and exchange and which serves as a hub for protecting thousands of various clients is capable of operation in a 24/7 mode. For this purpose, one must take care of ensuring backup power in case of a situation when centralised electrical supply is lost.

1.4. Securing against unwanted persons

1. For the purpose of monitoring doors, which lead to the security guard management centre and auxiliary premises, as well as

[453] Regulations of the Cabinet of Ministers No. 757. Regulations on the licensing of security guard activities. Adopted on 09.12.2014. *Latvijas Vēstnesis,* No. 257 (5317), 30.12.2014, Article 2

windows and the room housing UPS and the fuel power generator, reception antennas for security guard technical system signals and masts, the centre is equipped with video surveillance cameras. Video surveillance data are stored and kept for at least three months;

2. The alarm button is located at the workplace of a staff member on duty or is constantly by him/her. If the button is engaged, the alarm signal is received by an employee of the commercial provider of security guard services who ensures a 24-hour guarding at a post located outside the security guard management centre/control room;
3. The security guard management centre is equipped with communication devices for keeping contact with other members of the security staff, mobile groups of the commercial security service provider, and with other persons and institutions. Communication information is recorded and is stored for at least three months.[454]

While taking care of the property of others, commercial security guard service providers often forget about themselves and their own employees. It is important not to forget about the security of the security guard management centre/control room. In this regard we suggest taking several organisational actions:

1) to connect an alarm button at the security guard management centre/control room not just for the reaction of one's own security guard staff, but also for the staff of a cooperation partner;

[454] Regulations of the Cabinet of Ministers No. 757. Regulations on the licensing of security guard activities. Adopted on 09.12.2014. *Latvijas Vēstnesis*, No. 257 (5317), 30.12.2014, Article 2

2) to maintain regular contacts with an employee/-s of the security guard management centre/control room, e.g. a mobile group staff member perform hourly check-ups by radio or by mobile phone;
3) to conduct regular training courses for all employees of the security guard management centre/control room simulating various emergency situations – fire, loss of electrical power, armed attack, etc.;
4) to keep a spare access key or access card at a particular place.

The aforementioned requirements have been established by the regulations of the Cabinet of Ministers and are binding for commercial entities engaged in technical guarding of security guard management centres/control rooms. If a company has established its own internal security guard management centre/control room, it is advisable to observe the above-mentioned requirements to a maximum extent. This would make the local security guard management centre/control room more secure.

Although the regulations of the Cabinet of Ministers are not a complete copy of European normative acts, they include part of the EU legislation and do not contradict them. The requirements of the European standard NE 50518-1:2013 “Monitoring and alarm receiving centre” are much more strict. Currently, there are only a few companies in Latvia, which have fulfilled all the requirements and have qualified for this standard. Standard NE 50528 consists of three parts:

1) Location and construction requirements;
2) Technical requirements;
3) Procedures and requirements for operations.

A security guard management centre/control rooms represent good practice not just at security guard service companies or at protected facilities. Setting up of such a structure is highly important also at mass events. Setting up a control room at large mass events would assist in taking an effective care about the safety and security of visitors and guests. Normally, such centres are occupied not only by security guard staff, but also by representatives of national security structures, thus allowing to communicate in a fast and effective manner and to take all the necessary decisions.

Conclusions

The requirements of the European standard NE 50518-1:2013 “Monitoring and alarm receiving centre” are not freely available to any interested party. The regulations on the licensing of security guard activities mostly describe technical requirements for security guard management centres/control rooms.

Based on the conclusions, it is necessary to make the requirements of the European standard NE 50518-1:2013 “Monitoring and alarm receiving centre” freely available to any interested party, thus allowing commercial agents engaged in constructing a control room to compare their approach with the European standard. It would be equally important to their clients in order to make sure that the commercial agent engaged is prepared to operate according to high standards. It is also necessary to describe the procedural requirements making commercial agents engaged in providing security guard services act in a similar manner and clients would know what to expect from commercial agents.

References

Regulations of the Cabinet of Ministers No. 757. Regulations on the licensing of security guard activities. Adopted on 09.12.2014. *Latvijas Vēstnesis,* No. 257 (5317), 30.12.2014.

About the Authors

Uģis Začs, MBA
Uģis Začs received a Master's Degree in Business administration at the Riga Business School in 2015 and Bachelor's Degree in Regional development and governance at the Latvian University of Agriculture in 2011.
The author works in one of the largest security companies in Baltic States – SIA GRIFS AG – since 2006. The author works as a corporate client security manager and in his daily life deals with physical and technical security, manages different kind of objects, develops security concepts, and controls the security status of facilities. The author is also a lecturer at the Turība University, the programme on Company Security.

Dzintars Rendenieks, Student of Turiba University professional bachelor study program "Organization security"

Part VI

Cybersecurity

CYBERSECURITY AND RESILIENCE IN A SOCIETY

Julia Nevmerzhitskaya
Jyri Rajamäki

Introduction

Cybersecurity plays an important role in the field of information technology, but it also is one of the biggest challenges of today's life. In the recent years, the Internet and cyberspace has had a tremendous impact on all parts of society. Our daily life, fundamental rights, social interactions and economies depend on information and communication technology working seamlessly.[455] Digitalization, and more specifically open cyberspace promoted globalization and broke down barriers between countries and people, allowing free commerce and share of information and ideas.

Technologies allow us to connect networks and devices through the IoT and sensors, and share personal and business data anywhere and anytime. However, while the digital world brings enormous benefits, it is also vulnerable to threats. While Internet became the major part of our daily lives and the landscape of business operation, the question of securing the data, and ensuring its privacy, is of paramount importance. However, it is also important to remember that cybersecurity is not limited to securing information in IT networks. Cybersecurity is about *securing things*

[455] Joint Communication (2013). Joint communication to the european parliament, the council, the european economic and social committee and the committee of the regions Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace. Retrieved from https://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX:52011DC0303

that are vulnerable through ICT. In practice, it means that everything and everyone that can be accessed through cyberspace, devices and humans included. In this respect, one can argue that because of the digitalization everything becomes vulnerable. Our smart watches, mobile phones, and even health and wellbeing devices can be a source of vulnerability, exposing our private information. In this light, the role of cybersecurity is to protect what can be protected because of the security challenges posed by the use of ICT.

Cybersecurity concerns the whole of society. It is a shared responsibility of individuals, organizations, and different stakeholders working together to achieve safe and resilient societies. The challenges of the cybersecurity area are shared within countries and continents, and security incidents happening in one country can affect people all over the globe and disrupt functioning of a society's most critical services, such as energy and healthcare.

The rest of the article is structured as follows: in the first part, we introduce cybersecurity as a societal challenge, and describe major cyber threats affecting our society, and their implications to individuals, industries, and nations. The second part addresses the ways societies can deal with cyber threats, by introducing the concept of cyber resilience. In the last part, we provide recommendations to raise cyber awareness and basic cyber hygiene skills.

1. Understanding cybersecurity as a societal challenge

1.1. Cybersecurity terminology

Often the terms “information security” and “cybersecurity” are used as synonyms. Indeed, while many cybersecurity incidents are related to data breaches, it is important to understand that cybersecurity is a wider phenomenon. To understand the scope of cybersecurity and its impact on a society, first we introduce the main concepts based on ENISA report on definitions of cybersecurity[456] and NIST Glossary of Key Information Security Terms[457]:

The term “**security**” addresses the intent, such as being protected from personal and organisational data related dangers and threats; the term “security” can be used to refer to protection against undesirable data related threats.

The term “**cyberspace**” refers to the set of links and relationships between objects that are accessible through a generalised telecommunications network and to the set of objects themselves where they present interfaces allowing their remote control, remote access to data, or their participation in control actions within that cyberspace.

The term “**cybersecurity**” refers to security of cyberspace, and it means the ability to protect or defend the use of cyberspace from cyber attacks

[456] ENISA (2016). Definition of Cybersecurity – Gaps and overlaps in standardisation. Retrieved form https://www.enisa.europa.eu/publications/definition-of-cybersecurity

[457] NIST (National Institute of Standard and Technology) (2013). Glossary of Key Information Security Terms. Retrieved from http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf

The term "**information security**" refers to the protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.

The term "**resilience**" means ability to recover from or easily adjust to misfortune or change. In systems that provide critical services, resilience is characterized by four abilities: to plan/prepare, absorb, recover from, and adapt to known and unknown threats.

The term "**cyber threat**" refers to the possibility of a malicious attempt to damage or disrupt a computer network or system, including an attempt to access files and infiltrate or steal data.

Finally, the term "**vulnerability**" means any type of weakness in a computer system itself, in a set of procedures, or in anything that leaves information security exposed to a threat.

From a societal point of view it is important to recognize the differences, because cybersecurity addresses also the assets other than information that need to be protected. These assets can include a person himself, household appliances, medical devices, and interests of a society as a whole, in the areas of critical infrastructure. As presented in Figure 1, cybersecurity includes anyone or anything that can be reached via cyberspace.

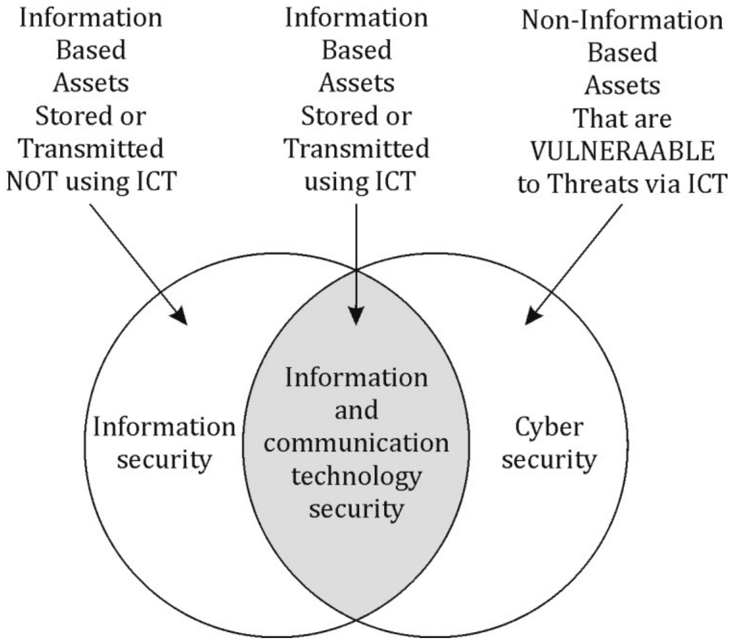

Information Based Assets Stored or Transmitted NOT using ICT
Information Based Assets Stored or Transmitted using ICT
Non-Information Based Assets That are VULNERAABLE to Threats via ICT
Information security
Information and communication technology security
Cyber security

Figure 1. **Information Security and Cybersecurity**[458]

1.2. Cyber–Physical Society and Critical Infrastructure

According to the Networking and Information Technology Research and Development (NITRD) "Cyber Physical Systems are smart networked systems with embedded sensors, processors and actuators that are designed to sense and interact with the physical world (including the human users), and support real-time, guaranteed performance in safety-critical applications. In CPS systems, the joint behaviour of the "cyber" and "physical" elements of the system is critical – computing, control, sensing and networking can be deeply

[458] Von Solms R., Van Niekerk J. (2013). From information security to cyber security. *Computers & Security*, Volume 38, October 2013, p. 97–102

integrated into every component, and the actions of components and systems must be safe and interoperable.“[459]

With the increasing digitalization in every aspect of our lives, and adoption of Internet of Things (IoT), not only computers but also other physical devices (such as for example household appliances) become interconnected. It means that physical and cyber spaces become intertwined, forming cyber-physical systems. IoT results in a cyber–physical society or what we also call a smart city (Figure 3). A cyber–physical society goes beyond the cyber space and includes interactions of humans and machines efficiently sharing resources in cyberspace, physical space and social space.

Understanding of cyber–physical system is especially important when it comes to critical infrastructure protection. European Commission defines critical infrastructure as an asset or system which is essential for the maintenance of vital societal functions. The damage to a critical infrastructure, its destruction or disruption by criminal activity or malicious behaviour, may have a significant negative impact for the security of the EU and the well-being of its citizens.[460] Critical infrastructure is harder to protect than information security due to its complexity.

[459] NIRD (2015). Cyber Physical Systems. Retrieved from https://www.nitrd.gov/nitrdgroups/images/6/6a/Cyber_Physical_Systems_%28CPS%29_Vision_Statement.pdf

[460] European Commission. (2018). Critical infrastructure. Retrieved from https://ec.europa.eu/home-affairs/what-we-do/policies/crisis-and-terrorism/critical-infrastructure_en

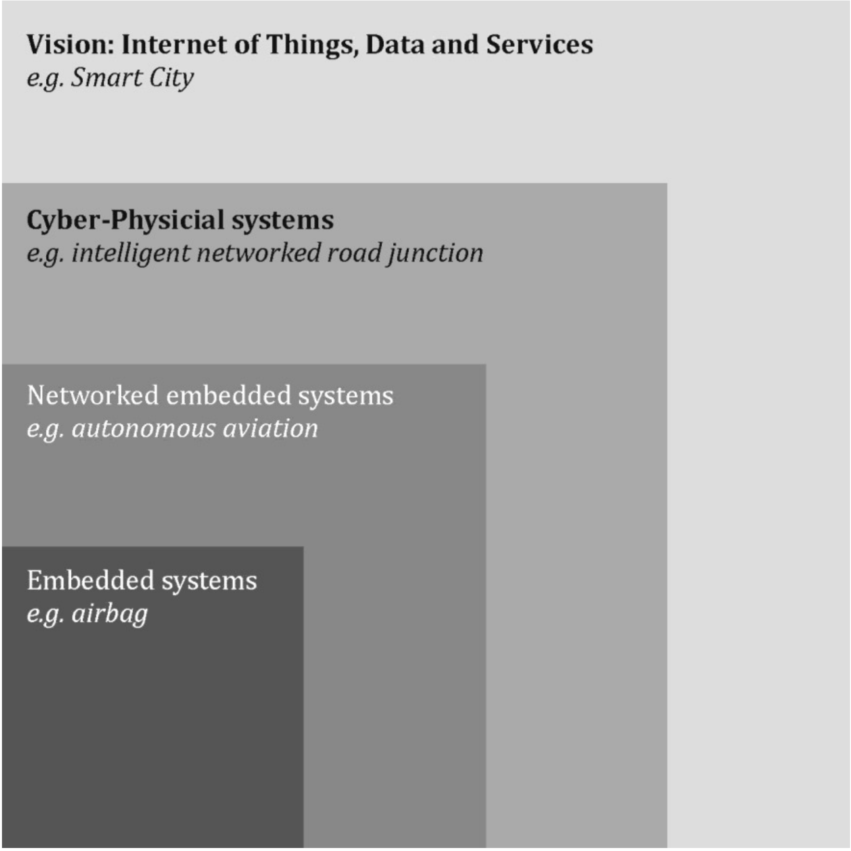

Vision: Internet of Things, Data and Services
e.g. Smart City
Cyber-Physicial systems
e.g. intelligent networked road junction
Networked embedded systems
e.g. autonomous aviation
Embedded systems
e.g. airbag

Figure 2. **Evolution of cyber physical systems**[461]

1.3. Cyber–threats and challenges

Resilience of a society depends on its ability to recover from damage or threat. For that, we need to understand first the nature and emerging trends in cyber threats. As defined earlier, a cyber-threat

[461] Acatech (Ed.) (2011). *Cyber-physical Systems. Driving Force for Innovation in Mobility, Health, Energy and Production Acatech* (ed.). Springer-Verlag Berlin Heidelberg

is a malicious act that attempts to gain access to a computer network without authorization or permission from the owners. There are different types of cyber threats, depending on the source of a threat, a target of the attack, and the type of the asset under the attack.

Outsider and insider threats

Most of the cybersecurity actions are targeted at securing assets from the threats coming from the hackers, or attackers, from the outside of organizations. Most commonly known outsider threats include *malware*, which is a broad class of attacks penetrating the system, usually without the owner being aware of the attack happening. In the recent years ransomware as a form of malicious attack has increased. Two most outstanding attacks in 2017 were wide-spread ransomware viruses known as WannaCry, and NotPetya.

Attackers can also be the insiders. Insider threats come from those who intentionally or non-intentionally cause damage by their behaviour, usually cause by non-compliance to organizational security policies. In fact, a growing number of cyber attacks and data breaches is associated with insider threats.[462] Insiders have easier access to organizational resources and system account, making it harder to monitor and prevent the attack.

Planned and unplanned threats

Planned threats are targeted attacks, usually with opportunistic goals (such as financial benefits, for example by demanding ransom to be paid, or by stealing and selling data). Planned attacks include cyber crime, cyber terrorism, hacking groups. One of the major threats

[462] Jang-Jaccard, J., Nepal, S. (2014). A survey of emerging threats in cybersecurity. *Journal of Computer and System Sciences*, No. 80 (2014) 973, August, p. 973–993

to a society are organized attacks to societal critical infrastructure. Often attackers are highly skilled, and supported by governments.

Unplanned attacks include actions by individuals (hackers) who exploit vulnerabilities in a system, as well as threats caused by the human factor (for example, an individual's behaviour in social media that results in exposing personal or sensitive information).

Threats to data and to devices

Finally, while in most cases the primarly target of the attack is information, with the rise of IoT and connected devices a number of cyber attacks directed at mobile devices, networked devices and sensors, focused on malfunction of a device, or denyal of a service. Such attacks can have a devastating impact on individuals (for example, in case of a malfunctioning medical device), organizations and a whole society, in case if attack is targeted at energy grids or other critical infrastructure. As stated in the ESET report on Cybersecurity trends 2018, "as everything gets smarter, the number of services that might be distupted by malware becomes greater."[463]

2. Building cyber resilience

2.1. Creating cyber awareness

Reducing the vulnerabilities of critical infrastructure and increasing their resilience is one of the major objectives of the EU. An adequate level of protection must be ensured and the detrimental effects of disruptions on the society and citizens must be

[463] ESET (2018). Cybersecurity trends 2018: The cost of our connected world, ESET. Retrieved from https://cdn1.esetstatic.com/ESET/US/resources/white-papers/ESET_Trends_Report_2018_final.pdf

limited as far as possible.[464] Enhancing cybersecurity and resilience starts with communicating the challenges and opportunities of cyber space to the society. The challenge, however, in creating cyber awareness, lies in a multi-disciplinary nature of cybersecurity. The scope of cybersecurity includes technical, organizational, economical, legal, societal and national security aspects, especially in the case of critical infrastructure protection.

Despite the growing number of threats and cyber attacks, awareness and knowledge of cybersecurity issues is still insufficient.[465] It is estimated that over two thirds of EU companies have no or basic understanding of their exposure to cyber risks, and over half of all European citizens feel not at all or not well informed about cyber threats. These figures correspond to the fact that the biggest risks are coming from the exploitation of human behaviour and they include sharing too much on social media, poor password security, and not realizing you are an attack target.[466]

Cybersecurity awareness is one of the parameters that is fundamental to fully achieving protection of cyber space. The purpose of cybersecurity awareness is to focus societal attention on security. Awareness raising responsibilities are shared on EU level by ENISA, Europol, and national data protection authorities. European Cybersecurity Organization (ECSO) sets awareness-raising and basic hygiene skills as one of the goals of the Work Group on cybersecurity

[464] European Commission. (2018). Migration and Home Affairs. Critical infrastructure. Retrieved from https://ec.europa.eu/home-affairs/what-we-do/policies/crisis-and-terrorism/critical-infrastructure_en

[465] European Commission. (2017). Cybersecurity. Resilience, Deterrence and Defence: Building strong cybersecurity in Europe

[466] Spitzner L. (2018). 2018 SANS Security Awareness Report: Building Successful Security Awareness Programs. Retrieved from https://www.sans.org/security-awareness-training/reports/2018-security-awareness-report

education and training.[467] Awareness is also included in the strategic guidelines of the Finnish Cybersecurity strategy.[468]

2.2. Towards resilient societies

The goal of cybersecurity is to build resilient societies. To achieve this goal, a nation needs to develop cyber capabilities, implement effective accountability, and be prepared and able to enter recovery at any time. In order for a society to be resilient, every system should identify four event management cycles (Figure 3): 1) Plan/Prepare: Lay the foundation to keep services available and assets functioning during a disruptive event (malfunction or attack); 2) Absorb: Maintain most critical asset function and service availability while repelling or isolating the disruption; 3) Recover: Restore all asset function and service availability to their pre-event functionality; 4) Adapt: Using knowledge from the event, alter protocol, configuration of the system, personnel training, or other aspects to become more resilient.

[467] European Cyber Security Organization (ECSO). (2018). WG5: Education, awareness, training, cyber ranges. Retrieved from http://www.ecs-org.eu/working-groups/wg5-education-awareness-training-cyber-ranges

[468] Finland's Cyber Security Strategy. (2013). Release: The Finnish cyber security strategy will be updated. Retrieved from https://turvallisuuskomitea.fi/index.php/fi/?option=com_dropfiles&format=&task=frontfile.download&catid=18&id=10&Itemid=1000000000000

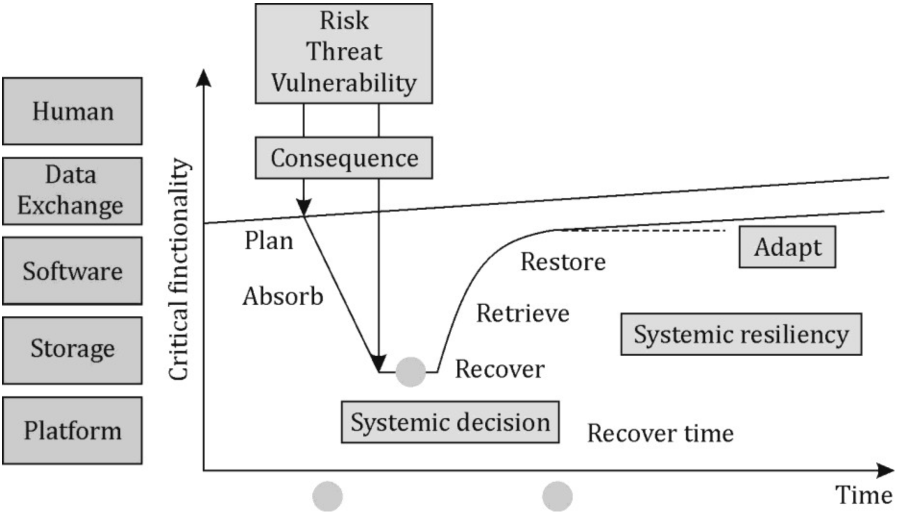


Figure 3. **Resilient societies**

Conclusions

Cybersecurity is a complex multidisciplinary phenomenon that affects individuals, organizations and societies, and includes technological, economic, legal, organizational aspects, as well as national security. With the growing digitalisation of our society and its vital services it is important to understand that cybersecurity is a shared responsibility, and it depends not only on security providers, but also on our individual behaviour.

From a societal point of view, the biggest threats are caused by new trends in cyber-physical systems and beyond, including Internet of Things and connected devices. These connected physical and cyber spaces create a good platform for cyber attacks, which can be devastating when effecting such critical societal services as energy grids, healthcare or water supply. We have witnessed a wide-spread malicious attacks on critical infrastructure a number of times in the last years, and the amount of attacks is likely to increase in the following years. These attacks can target an information, but they can also cause disruption in the functioning of devices and services.

Understanding the consequences of cyber-attacks to a critical infrastructure requires a shared responsibility among national and local entities, public and private owners and operators, and the IT hardware and service providers. This shared responsibility is a key to achieving cyber resiliency in a society, in order to prepare for, adapt to changing conditions, and recover from cyber–attacks. Building cyber resilient societies starts with raising awareness about cybersecurity among individuals. With majority of the cybersecurity incidents being caused by human factor, it is of outmost importance to communicate cybersecurity risks and impacts in a clear and understandable way. In addition to raising awareness, each nation needs to develop cyber capabilities and be prepared to recover from cyber incidents, and learn and adapt.

References

Acatech (Ed.). (2011). *Cyber-physical Systems. Driving Force for Innovation in Mobility, Health, Energy and Production Acatech* (ed.). Springer-Verlag Berlin Heidelberg

Jang-Jaccard, J., Nepal, S. (2014). A survey of emerging threats in cybersecurity. *Journal of Computer and System Sciences*, No. 80 (2014) 973, August, p. 973–993

Spitzner, L. (2018). 2018 SANS Security Awareness Report: Building Successful Security Awareness Programs. Retrieved from https://www.sans.org/security-awareness-training/reports/2018-security-awareness-report

Von Solms, R., Van Niekerk, J. (2013). From information security to cybersecurity, *Computers & Security*, Volume 38, October, p. 97–102

Joint Communication (2013). Joint communication to the European parliament, the council, the European economic and social committee and the committee of the regions Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace. Retrieved from https://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX:52011DC0303

ENISA. (2016). Definition of Cybersecurity – Gaps and overlaps in standardisation. Retvieved form https://www.enisa.europa.eu/publications/definition-of-cybersecurity

European Commission (2018). Critical infrastructure. Retrieved from https://ec.europa.eu/home-affairs/what-we-do/policies/crisis-and-terrorism/critical-infrastructure_en

European Commission (2017). Cybersecurity. Resilience, Deterrence and Defence: Building strong cybersecurity in Europe

ESET (2018). Cybersecurity trends 2018: The cost of our connected world, ESET. Retrieved from https://cdn1.esetstatic.com/ESET/US/resources/white-papers/ESET_Trends_Report_2018_final.pdf

European Commission (2018). Migration and Home Affairs. Critical infrastructure. Retrieved from https://ec.europa.eu/home-affairs/what-we-do/policies/crisis-and-terrorism/critical-infrastructure_en

European Cybersecurity Organization (ECSO). (2018). WG5: Education, awareness, training, cyber ranges. Retrieved from http://www.ecs-org.eu/working-groups/wg5-education-awareness-training-cyber-ranges

Finland's Cybersecurity Strategy (2013). Release: The Finnish cybersecurity strategy will be updated. Retrieved from https://turvallisuuskomitea.fi/index.php/fi/?option=com_dropfiles&format=&task=frontfile.download&catid=18&id=10&Itemid=1000000000000

NIRD (2015). Cyber Physical Systems. Retrieved from https://www.nitrd.gov/nitrdgroups/images/6/6a/Cyber_Physical_Systems_%28CPS%29_Vision_Statement.pdf

NIST (National Institute of Standard and Technology). (2013). Glossary of Key Information Security Terms. Retrieved from http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf

About the Authors

Jyri Rajamäki, *Adjunct Professor, Dr.*

Dr. Rajamäki holds *M.Sc.* degree (1991) in electrical engineering from Helsinki University of Technology, *Lic.Sc*. (2000) and *D.Sc.* (2002) degrees in electrical and communications engineering from Helsinki University of Technology, and PhD degree (2014) in mathematical information technology from University of Jyväskylä.

Since 2006, Dr. Rajamäki has been Principal Lecturer in Information Technology at Laurea University of Applied Sciences (UAS), Finland. Currently, he is also Adjunct Professor of Critical Infrastructure Protection and Cybersecurity at the University of Jyväskylä. Dr. Rajamäki worked ten years (1986–1996) for Telecom Finland, main tasks being uninterruptible power supplies, electromagnetic compatibility (EMC), and electromagnetic pulse protection. From 1996 to 2006, Dr. Rajamäki acted as Senior/Chief Engineer for Safety Technology Authority of Finland where his main assignment was to make the Finnish market ready for the European EMC Directive. Dr. Rajamäki was 17 years the secretary or a member of Finnish national standardization committee on EMC, and he represented 15 years Finland at IEC, CISPR, CENELEC and ETSI EMC meetings. He was the Chairman of Finnish Advisory Committee on EMC from 1996 to 2006. The head of Data Networks Lab of Laurea UAS. Dr. Rajamäki has been the scientist in charge, national coordinator and scientific supervisor for several national and European research projects. For the European Research Area he has acted as the evaluator of the projects, and being an advisor board member of the FP7 Projects.

Julia Nevmerzhitskaya, Senior Lecturer, RD&I
Nevmerzhitskaya has two master degrees (*M.Sc* (Econ) 1998, *M.Sc* (Hospitality Management) 2013), and continuing her studies as a PhD candidate from University of Vaasa, Doctoral school of Marketing. Julia also completed Professional Pedagogical Degree in 2008 and she is a qualified professional teacher.
Julia has over 14 years of working in higher education, teaching in a number of Bachelor and Master degrees subjects related to service management and marketing. Since 2014 she is a member of Laurea UAS's Research, Development and Innovation unit, concentrating on development projects in Service Business, and Cybersecurity. She is representing Laurea at European Organization for Security (EOS) Cybersecurity Work Group, and European Cybersecurity Organization (ECSO) Strategic Research and Innovation Agenda (SRIA).

CYBERSECURITY IN AN ORGANIZATION

Jyri Rajamäki,
Julia Nevmerzhitskaya

Introduction

The aim of cybersecurity is to make cyber space safe from damage or threat. Figure 1 shows three perspective views of cyber space: (1) data or information perspective that comes from the information theory space; (2) technology perspective that includes the hardware, silicon, and wires, as well as software, operating systems, and network protocols; and (3) human perspective that acknowledges that the human is as much responsible for the dynamics of the system as is the data and the technology.[469]

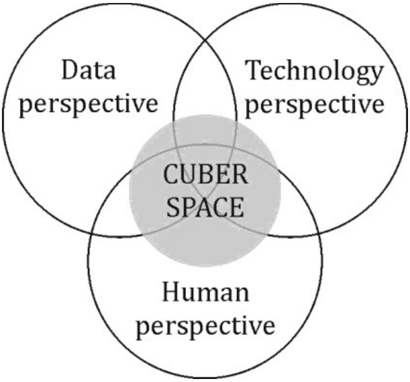


Figure 1. **Cyber space at the overlap of data, technology and human**[470]

[469] Edgar, T., & Manz, D. (2017). *Research methods for cyber security*. Cambridge: Syngress

[470] Ibid

From an organization's point of view, cybersecurity management starts by a risk management procedure, as shown in Figure 2. If cybersecurity risks are not made ready, organizations will face severe disasters over time. Risk management research focuses on how to measure and quantify a state of cybersecurity, including quantifying the value of cybersecurity to an operation, how much of a threat is the operation exposed to, and scoring how mitigations and security controls affect the overall operational risk.[471] All organizations are becoming more and more dependent on unpredictable cybersecurity risks. Everywhere present computing means that organizations do not know when they are using dependable devices or services and there are chain reactions of unpredictable risks.

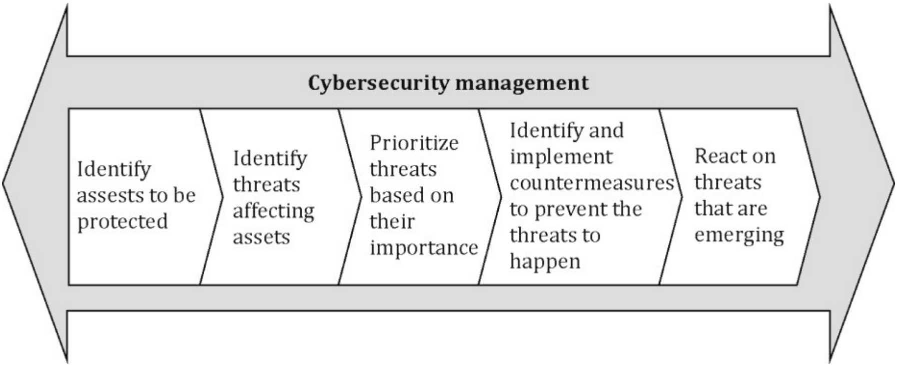

Cybersecurity management
Identify assests to be protected
Identify threats affecting assets
Prioritize threats based on their importance
Identify and implement countermeasures to prevent the threats to happen
React on threats that are emerging

Figure 2. **Cybersecurity management as a risk management procedure**[472]

[471] Edgar, T., & Manz, D. (2017). *Research methods for cyber security*. Cambridge: Syngress

[472] Kataikko, M. (2017). *Cyber Security In Health Care: From Threat To Opportunity*. Jyväskylä: Business JKL

1. Building Cyber–Trust

The purpose, with regard to security, is to know what is going on and what will happen in the network(s), and to be aware of the current level of security in the network(s), how to design or build-in security and resilience to a networked environment, and to define trade-offs for security and privacy levels versus system's usability.[473] The overall aim is to mitigate cybersecurity risks, which in its turn supports the business continuity and operations of the whole society.[474]

Investing in systems that improve confidence and trust can significantly reduce costs and improve the speed of interaction. From this perspective, cybersecurity should be seen as a key enabler for the development and maintenance of trust in the digital world. Cybersecurity has the following four themes: (1) security technology, (2) situational awareness, (3) security management, and (4) resilience[475], as shown in Figure 3. Situational awareness is needed for having a correct understanding of security incidents, network traffic, and other important aspects that affect security; and security technologies are needed for protection.[476] Human aspects have to rule in via security management.[477] Consequently,

[473] Ahokangas, M., Arkko, V., Aura, T., Erkinheimo, P., Evesti, A., Frantti, T., Hautamäki, J., Helenius, M., Hämäläinen, M., Kemppainen, J., Kirichencko, A., Korkiakoski, M., Kuosmanen, P., Laaksonen, M., Lehto, M., Manner, J., Remes, J., Röning, J., Sahlin, B., Savola, R., Seppänen, V., Sihvonen, M., Tsochou, A. & Vepsäläinen, P. (2014). *Strategic research agenda for cyber trust*. DIGILE

[474] DIGILE (2014). In the pipeline: Cyber trust. Retrieved form: http://www.digile.fi/Services/researchprograms/cybertrust

[475] Ahokangas, M., et al. (2014). Strategic research agenda for cyber trust. DIGILE

[476] Ibid

[477] Rajamäki, J., Rajamäki, M. (2013). National Security Auditing Criteria, KATAKRI: Leading Auditor Training and Auditing Process. *12th European Conference on Information Warfare and Security, Academic Conferences and Publishing International Limited*, Reading, pp. 217–223

resilient systems and infrastructures have the ability to prepare and plan for, absorb, recover from, and more successfully adapt to adverse events.[478] Security audit is a way to demonstrate an organization's security level.

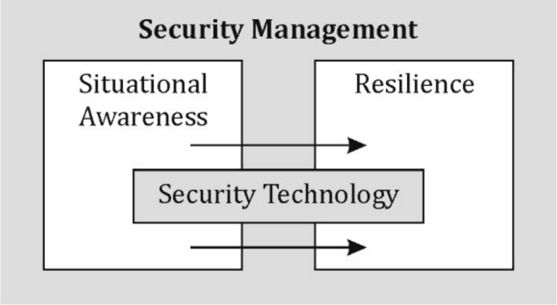


Figure 3. **Themes of Trust-building**[479]

1.1. Resilience

The human body is inherently resilient in its ability to persevere through infections or trauma, but our society's critical infrastructure lacks the same degree of resilience, typically losing essential functionality following adverse events.[480] Without proper protection and development with cybersecurity in mind, modern society relying on critical infrastructures would be extremely vulnerable to accidental and malicious cyber threats. Resilient systems

[478] National Research Council (2012). Disaster Resilience: A National Imperative. The National Academies Press

[479] Adopted from Ahokangas, M., et al. (2014). *Strategic research agenda for cyber trust*. DIGILE

[480] Linkov, I., Bridges, T., Creutzig, F., Decker, J., Fox-Lent, C., Kröger, W., Lambert, J. H., Levermann, A., Montreuil, B., Nathwani, J., Nyer, R., Renn, O., Scharte, B., Scheffler, A., Schreurs, M. & Thiel-Clemen, T. (2014). Changing the resilience paradigm. *Nature Climate Change*, 4, pp. 407–409

are able to minimize the negative impacts of adverse events on societies and sustain or even improve their functionality by adapting to and learning from fundamental changes caused by those events.[481]

The overall target of cybersecurity is that systems and infrastructures are resilient against all cyber incidents. In the case of information security, resilience means that a system or infrastructure is able to adapt to changing conditions, based on run-time situational awareness and a priori risk analysis.[482] Resilience is based on integrating two parallel subtasks: (1) run-time situational awareness and (2) a priori risk analysis. On the other hand, resilience itself is a twofold topic: (1) the system has to be robust against attacks, i.e., the attack is prevented in its first phase, and (2) the system has to be able to return to a safe state after the attack. Healing requires that utilized data and system operation can be restored as soon as possible. Therefore, healing processes have to be trained and tested.

1.2. Situational Awareness

Situational Awareness is the main prerequisite towards cybersecurity. Without situational awareness, it is impossible to systematically prevent, identify, and protect the system from the cyber incidents and if, for example, a cyber-attack happens, to recover from the attack.[483] Situational awareness involves being aware of what is happening around your system to understand how

[481] Linkov, I., Bridges, T., Creutzig, F., Decker, J., Fox-Lent, C., Kröger, W., Lambert, J. H., Levermann, A., Montreuil, B., Nathwani, J., Nyer, R., Renn, O., Scharte, B., Scheffler, A., Schreurs, M. & Thiel-Clemen, T. (2014). Changing the resilience paradigm. *Nature Climate Change*, 4, pp. 407–409

[482] Ahokangas, M., et al. (2014). *Strategic research agenda for cyber trust*. DIGILE

[483] Ibid

information, events, and how your own actions affect the goals and objectives, both now and in the near future. It also enables to select effective and efficient countermeasures, and thus, to protect the system from varying threats and attacks.

Situational awareness is needed for creating a sound basis for the development and utilization of countermeasures (controls), where resilience focuses. The most important enablers of situational awareness are observations, analysis, and visualization, cyber-policy of the government as well as national and international cooperation. For the related decision-making, relevant information collected from different sources of the cyber environment or cyberspace, e.g., networks, risk trends, and operational parameters, are needed. This requires information exchange between different stakeholders. And always, when dealing with information exchange, the main question is "trust".

1.3. Security technology

Security technologies include all technical means towards cybersecurity, such as secure system architectures, protocols and implementation, as well as tools and platforms for secure system development and deployment. Security technologies are needed for fulfilling the recognized security requirements, and for building resilient infrastructures and systems with dependable hardware and software that can also meet future security challenges.[484]

Security technologies enable technical protection of infrastructures, platforms, devices, services, and data. The technical protection starts with secure user identification and authorization that are necessary features in most secure infrastructures, platforms, devices

[484] Ahokangas, M., et al. (2014). *Strategic research agenda for cyber trust*. DIGILE

and services. Fortunately, well-known technologies exist for their implementation. Typically, processes and data objects are associated with an owner, represented in the computer system by a user account, who sets the access rights for others. A global trend is to increase the use of cloud service technology when providing critical services. Data go into a cloud and will not come back to end-users' devices. Also, government data has already gone to a cloud, and in the future more and more government data will migrate to cloud servers and services. Partnerships between cloud service providers and security solution providers are becoming more common. We will see the emergence of cloud service-specific-solution providers as well. Identity management and encryption will be the most important cloud security services to be offered. These services will be eventually offered for small to medium-sized businesses as well. We will also see emergence of cloud security standards. Challenges are that quite often cloud service providers believe that security is just an end user issue and firewall means security. Therefore, currently, we do not have proper cloud security standards and we lack awareness of a true understanding of comprehensive cloud security.[485]

Security technologies are needed also then if something has happened. For example, forensics can lead to the sources of the attack/mistake and provide information for legal and other ramifications of the issue. Forensics also facilitates the analysis of the causes of the incident, which in turn, makes it possible to learn and avoid similar attacks in the future.

[485] Ahokangas, M., et al. (2014). *Strategic research agenda for cyber trust*. DIGILE. In the pipeline: Cyber trust. Retrieved form: http://www.digile.fi/Services/researchprograms/cybertrust

1.4. Security management and governance

The well-known fact of life is that people are the rock-bottom of cybersecurity. Security management and governance, “the brain and Intelligence of cybersecurity” takes care of the human and organizational aspects of cybersecurity.

Security policy is currently the main element used to communicate secure work practices to employees and ICT stakeholders. It is a declaration of the significance of security in the business of the organization in question. Additionally, the security policy defines the organization’s policies and practices for personnel collaboration. However, people still often fail to comply with security policies, exposing the organization to various risks. One challenge is to promote methods and techniques that can support the development of comprehensible security policies in the emerging ICT paradigms, e.g., cloud computing and multiple devices.[486] Developing of policies that can defeat the main reasons driving non-compliance, such as a habit, is challenging.

Information security management system (ISMS) means continuously managing and operating system by documented and systematic establishment of the procedures and process to achieve confidentiality, integrity and availability of the organization’s information assets that do preserve.[487] ISMS provides controls to protect organizations’ most fundamental asset, information. Many organizations apply audits and certification for their ISMS to convince their stakeholders that security of organization is properly

[486] Ahokangas, M., et al. (2014). *Strategic research agenda for cyber trust*. DIGILE.

[487] Lee, W. & Jang, S. (2009). *A study on information security management system model for small and medium enterprises*. Recent advances in e-activities, information security and privacy, pp. 84–87

managed and meets regulatory security requirements.[488] An information security audit is an audit on the level of information security in an organization. Security aware customers may require ISMS certification before business relationship is established. Unfortunately, ISMS standards are not perfect and they possess potential problems. Usually guidelines are developed using generic or universal models that may not be applicable for all organizations. Guidelines based to common, traditional practices take into consideration differences of the organizations and organization specific security requirements.[489]

2. Security audit

Many different types of audits exist, including financial audits, property assessments, supplier reviews, contractor evaluations, registration audits and equipment evaluations.[490] Figure 4 illustrates internal (first-party) and external (second-party and third-party) auditing types. The common principle is that they compare applied procedures, as well as a set of collected information, against some established criteria.

[488] Broderick, J. S. (2006). ISMS, security standards and security regulations. *Information security technical report*, 11 (1), pp. 26–31

[489] Siponen, M., Willison, R. (2009). Information security management standards: Problems and solutions. *Information & Management,* No. 46 (5), pp. 267–270

[490] Russell, J. P. (2012). *The ASQ auditing handbook*. ASQ Quality Press

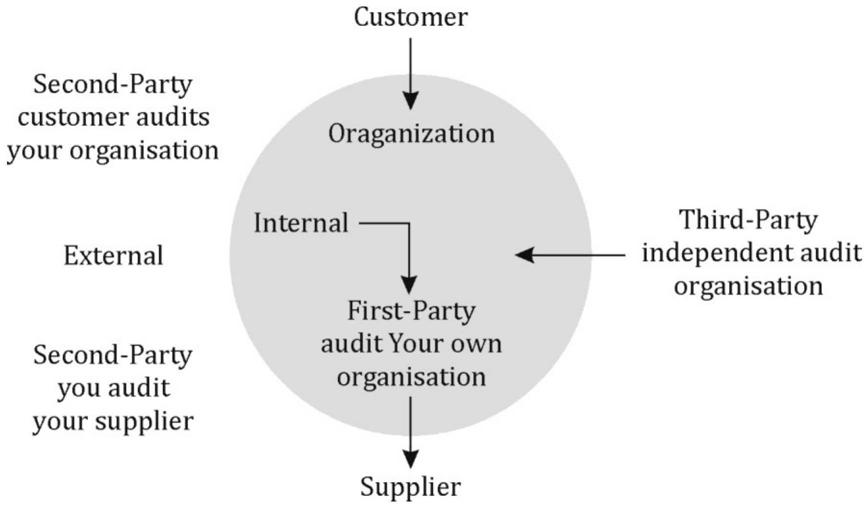

Customer
Second-Party customer audits your organisation
Oraganization
Internal
External
Third-Party independent audit organisation
First-Party audit Your own organisation
Second-Party you audit your supplier
Supplier

Figure 4. **Firs-second- and third-party audits**[491]

ISO/IEC 17021-2 is a normative standard intended for use by accreditation bodies when assessing management systems, while ISO 19011 provides guidelines for first-, second- and third-party auditors when auditing management systems. The third-party certification industry will use ISO 17021-2 to define requirements for audits and audit arrangements and accreditation bodies will determine whether a certification body's auditing arrangements and activities comply with those requirements. ISO 19011 identifies best practice and provides information on what should be done when carrying out an audit without specifying how it must be done. ISO 19011:2011 edition includes an extension of the standard's earlier scope of application from quality and environmental management systems to all types of management systems auditing. Continuing development of management systems standards for

[491] Adapted from: Russell, J. P. (2012). *The ASQ auditing handbook*. ASQ Quality Press

information security, for example, means that ISO 19011 must be able to accommodate differing requirements while still providing useful guidance.[492]

The three things that make a management system audit different from other types of assessments are that the audit must be (1) systematic, (2) independent and (3) documented. In order to conduct systematic management system audits, there is a need for both audit procedures and an audit programme. From an independence point of view, auditors cannot audit their own work or that of their colleagues', as there would be a conflict of interest. Audits need to be structured, to ensure they are free from bias and conflicts of interest. Audits must be documented, because they are all about making decisions and taking action.[493]

The root of the Finnish National Security Auditing Criteria, KATAKRI, is to preserve the confidentiality of any confidential and classified information held by the organization concerned. It is published by the Ministry of Defence, but Confederation of Finnish Industries, Finnish Communications Regulatory Authority (FICORA), Ministry of Foreign Affairs and Ministry of the Interior have also participated in the preparation of the criteria. KATAKRI was officially published in 2009, update in 2011, and Version III was published in March 2015.

The National Security Auditing Criteria are mutual security criteria for officials and companies for unifying the communal

[492] Simpson P. (2010). ISO 19011 vs ISO/IEC 17021-2. The Health and Safety Edition. INform 27. Retrieved form: http://www.irca.org/en-gb/resources/INform/archive/issue27/Features/Building-on-safety21/

[493] Rajamäki, J., Rajamäki, M. (2013). National Security Auditing Criteria, KATAKRI: Leading Auditor Training and Auditing Process. *12th European Conference on Information Warfare and Security*, Academic Conferences and Publishing International Limited, Reading, pp. 217–223

security procedures and to improve self-monitoring and auditing. The National Security Auditing Criteria are an auditing tool used by the officials when carrying out inspections on the level of security within a company or a community. According to the current version of the criteria, KATAKRI's main goal is to harmonize official measures when an authority conducts an audit in a company or in another organization to verify their security level. The Finnish National Security Authority uses KATAKRI as its primary tool when checking the fulfilment of security requirements. The preface to the criteria states that the second important goal is to support companies and other organizations, as well as authorities and their service providers and subcontractors, in working on their own internal security. For that reason, the criteria contain recommendations for the industry that are separate and outside of the official requirements; it is hoped that useful security practices will be chosen and applied, thus progressing to the level of official requirements.

The Finnish National Security Auditing Criteria, KATAKRI are divided into three main areas: (1) administrative and personnel security, (2) physical security, and (3) information security. Areas are not meant to be used independently. It is instructed to take all three areas into account when performing accreditation audit using KATAKRI.

Conclusions

Business continuity management and risk management systems are based on probabilistic quantitative methods and they are useful for dealing with foreseeable and calculable stress situations. However, they are no longer sufficient to address the evolving nature of risks in the modern cyber-physical world having non-foreseeable and non-calculable stress situations. Also, the high level of interconnectivity in modern society with complexities of large integrated cyber-physical systems (CPS) has opened many avenues for cyber-attacks. Therefore, the issue of cyber-security is currently having and will continue to have a major impact on all organizations and the whole organized society.

Safety and security thinking has been based on the supposition that we are safe and we are able to prevent “bad touch”. The focus of actions has been to control one’s own systems, to improve protection, and to stay inside this circle of protection. However, nobody alone is able to fully control complex large integrated cyber-physical systems; coordination and cooperation are needed. This means that the focus of cybersecurity education should shift from controlling and securing one’s own data to cooperation and information sharing between the different stakeholders which is the only way to promote more resilient complex systems of systems.

For the above mentioned reasons, we have an urgent need to complement the existing knowledge-base of business continuity and risk management by developing frameworks and models enabling network-wide resilience management (RM). In the future, RM should be used to allocate resources to enhance resilience.

References

Ahokangas, M., Arkko, V., Aura, T., Erkinheimo, P., Evesti, A., Frantti, T., Hautamäki, J., Helenius, M., Hämäläinen, M., Kemppainen, J., Kirichencko, A., Korkiakoski, M., Kuosmanen, P., Laaksonen, M., Lehto, M., Manner, J., Remes, J., Röning, J., Sahlin, B., Savola, R., Seppänen, V., Sihvonen, M., Tsochou, A. & Vepsäläinen, P. (2014). *Strategic research agenda for cyber trust*. DIGILE

Broderick, J. S. (2006). ISMS, security standards and security regulations. *Information security technical report*, No. 11 (1), pp. 26–31

DIGILE (2014). In the pipeline: Cyber trust. Retrieved form: http://www.digile.fi/Services/researchprograms/cybertrust

Edgar, T., & Manz, D. (2017). *Research methods for cyber security*. Cambridge: Syngress

Kataikko, M. (2017). *Cyber Security In Health Care: From Threat To Opportunity*. Jyväskylä: Business JKL

Lee, W. & Jang, S. (2009). A study on information security management system model for small and medium enterprises. Recent advances in e-activities, information security and privacy, pp. 84–87

Linkov, I., Bridges, T., Creutzig, F., Decker, J., Fox-Lent, C., Kröger, W., Lambert, J. H., Levermann, A., Montreuil, B., Nathwani, J., Nyer, R., Renn, O., Scharte, B., Scheffler, A., Schreurs, M. & Thiel-Clemen, T. (2014). Changing the resilience paradigm. *Nature Climate Change*, No. 4, pp. 407–409

National Research Council (2012). Disaster Resilience: A National Imperative. The National Academies Press

Rajamäki, J., Rajamäki, M. (2013). National Security Auditing Criteria, KATAKRI: Leading Auditor Training and Auditing Process. *12th European Conference on Information Warfare and Security*, Academic Conferences and Publishing International Limited, Reading, pp. 217–223

Russell, J. P. (2012). *The ASQ auditing handbook*. ASQ Quality Press

Simpson, P. (2010). ISO 19011 vs ISO/IEC 17021-2. The Health and Safety Edition. INform 27. Retrieved form: http://www.irca.org/en-gb/resources/INform/archive/issue27/Features/Building-on-safety21/.

Siponen, M., Willison, R. (2009). Information security management standards: Problems and solutions. *Information & Management,* No. 46 (5), pp. 267–270

Star, S. L., Ruhleder, K. (1996). Steps toward an ecology of infrastructure: Design and access for large information spaces. *Information systems research,* No. 7 (1), pp. 111–134

About the Authors

Jyri Rajamäki, Adjunct Professor*, Dr.*
Dr. Rajamäki holds *M.Sc.* degree (1991) in electrical engineering from Helsinki University of Technology, *Lic.Sc.* (2000) and *D.Sc.* (2002) degrees in electrical and communications engineering from Helsinki University of Technology, and PhD degree (2014) in mathematical information technology from University of Jyväskylä. Since 2006, Dr. Rajamäki has been Principal Lecturer in Information Technology at Laurea University of Applied Sciences (UAS), Finland. Currently, he is also Adjunct Professor of Critical Infrastructure Protection and Cybersecurity at the University of Jyväskylä. Dr. Rajamäki worked ten years (1986–1996) for Telecom Finland, main tasks being uninterruptible power supplies, electromagnetic

compatibility (EMC), and electromagnetic pulse protection. From 1996 to 2006, Dr. Rajamäki acted as Senior/Chief Engineer for Safety Technology Authority of Finland where his main assignment was to make the Finnish market ready for the European EMC Directive. Dr. Rajamäki was 17 years the secretary or a member of Finnish national standardization committee on EMC, and he represented 15 years Finland at IEC, CISPR, CENELEC and ETSI EMC meetings. He was the Chairman of Finnish Advisory Committee on EMC from 1996 to 2006. The head of Data Networks Lab of Laurea UAS. Dr. Rajamäki has been the scientist in charge, national coordinator and scientific supervisor for several national and European research projects. For the European Research Area he has acted as the evaluator of the projects, and being an advisor board member of the FP7 Projects.

Julia Nevmerzhitskaya, Senior Lecturer, RD&I
Nevmerzhitskaya has two master degrees (*M.Sc* (Econ) 1998, *M.Sc* (Hospitality Management) 2013), and continuing her studies as a PhD candidate from University of Vaasa, Doctoral school of Marketing. Julia also completed Professional Pedagogical Degree in 2008 and she is a qualified professional teacher.
Julia has over 14 years of working in higher education, teaching in a number of Bachelor and Master degrees subjects related to service management and marketing. Since 2014 she is a member of Laurea UAS's Research, Development and Innovation unit, concentrating on development projects in Service Business, and Cybersecurity. She is representing Laurea at European Organization for Security (EOS) Cybersecurity Work Group, and European Cybersecurity Organization (ECSO) Strategic Research and Innovation Agenda (SRIA).

CYBERSECURITY: HOW TO STAY SAFE IN THE CYBERSPACE

Elina Radionova-Girsa

Introduction

Is being digital in our everyday lives good or not? Of course, it is very easy and convenient to always be online – to be able to communicate, to study, to work, to do shopping, to watch movies and listen to music. And why not do that on the Internet. It is great when all information you need is saved on your devices. You can travel to another country and use a map which is connected to the Internet, you can park a car in a parking place and pay by downloading a special application and saving in it your credit card date, and so on. But on the other side is that safe? The author wants to pinpoint that being online is not so bad if you know how to deal with threats coming from cyberspace.

According to the Central Statistical Bureau of Latvia[494] in 2017 the Internet usage by individuals at the beginning of the year was 78.5 % of the total population. That number is quite massive. And talking about individuals who experienced security related incidents through using the Internet, it is possible to see that in Latvia in 2015 16.7 % of the Internet users had caught a virus or other computer infection (e.g. worm or trojan horse) resulting in loss of information or time, 1.4 % of the Internet users were abused of personal information sent on the Internet and/or other privacy violations, 1.1 % of children had accessed inappropriate websites,

[494] Central Statistical Bureau of Latvia (2018). Retrieved from http://www.csb.gov.lv/dati/statistikas-datubazes-28270.html

0.3 % and 0.2 % of the Internet users had financial loss due to fraudulent payment (credit or debit) card use and financial loss as a result of receiving fraudulent messages (phishing) or getting redirected to fake websites asking for personal information (pharming).[495] At the first sight those percentages are not so big but if we think about losses, not only financial but time and moral as well, we can understand the problem's limits.

Even the President of Latvia Raimonds Vējonis while visiting the Information Technology Security Incident Response Institution CERT.LV told: "Cybersecurity imposes one of the greatest challenges for the future not only on a state but also on every citizen. To overcome this challenge much has been already done at national level. However, to ensure the security of our information space and cybersecurity, the capacity of the responsible institutions must be further enhanced, and public media literacy must be facilitated."[496]

Such problems and issues are worldwide because of borderlessness of the cyberspace. In Europe 51 % of European citizens feel uninformed on cyber threats and 69 % of companies have no basic understanding of their exposure to cyber risks.[497] The main goal for the research is to find out the main cybersecurity approaches worldwide and compare it to the Baltic States regulations. It is needed to understand how countries adapt and integrate international legislation directly to their countries. Such methods as comparative

[495] Central Statistical Bureau of Latvia (2018). Retrieved from http://www.csb.gov.lv/dati/statistikas-datubazes-28270.html

[496] The President of Latvia: Cybersecurity is one of our greatest challenges for the future. (2018). Retrieved from https://www.president.lv/en/news/news/the-president-of-latvia-cybersecurity-is-one-of-our-greatest-challenges-for-the-future-25408

[497] European Council. (2017). Reform of cyber security in Europe. Retrieved from http://www.consilium.europa.eu/en/policies/cyber-security/

analysis of regulations on cybersecurity, scientific literature analysis and doctrinal analysis were used during the research. Results can be used both in a theoretical way and in practise in order to understand cybersecurity problems and the character of legal regulations among Baltic States Countries.

1. Cybersecurity

1.1. Cybersecurity issues

Cybersecurity meaning

Before you begin to think about how to protect yourself from cyber-attacks and take care of your own cybersecurity and your country's citizens, it's necessary to understand what exactly cybersecurity is. In many sources, both in books, in scientific articles, and in the websites of various state institutions, information is displayed that allows one to see not only the definition itself, but also the meaning and explanation which, in the author's opinion, are more important.

Cybersecurity is the practice of protecting systems, networks, and programs from digital attacks. These attacks are usually aimed at accessing, changing, or destroying sensitive information; extorting money from users; or interrupting normal business processes.[498]

Cybersecurity involves preventing, detecting, and responding to cyber incidents that can have wide ranging effects on the individual, organizations, the community and at the national level.[499] The Network and Information Security (NIS) directive *aims to harmonise*

[498] Cisco website (2018). Retrieved from https://www.cisco.com/c/en/us/products/security/what-is-cybersecurity.html

[499] Official website of the Department of Homeland Security (2018). Cybersecurity. Retrieved from https://www.ready.gov/cybersecurity

cybersecurity laws across Europe and improve cooperation on cybersecurity between EU countries. Anyone from individuals to companies and public authorities can fall victim to schemes such as identity theft, fake bank websites or industrial espionage.

The author would like to consider that all the definitions very well represent the main features of cybersecurity. The key point that is being highlighted is the security issue surrounding cyberspace and the risks involved.

According to a Eurobarometer survey published in February 2017, Europeans are highly concerned about cybersecurity: 89 % of all internet users avoid disclosing personal information online, while 85 % agree that the risk of becoming a victim of cybercrime is increasing. Every day more than 150,000 viruses and other malicious codes circulate.[500]

The author points to the fact that if the user is knowledgeable and educated about cybersecurity issues, then he will have much less risk than users who have little or no interest at all about such problems. It is also necessary to highlight the various types of threats to Internet users on a daily basis.

Cybercrime consists of criminal acts that are committed online by using electronic communications networks and information systems. It is a borderless problem that can be classified in three broad definitions:

1) crimes specific to the Internet, such as attacks against information systems or phishing (e.g. fake bank websites to solicit passwords enabling access to victims' bank accounts);

[500] European Parliament. (2018). Retrieved from http://www.europarl.europa.eu/news/en/headlines/society/20180514STO03405/pesticides-investigation-health-should-be-the-priority

2) online fraud and forgery. Large-scale fraud can be committed online through instruments such as identity theft, phishing, spam and malicious code;
3) illegal online content, including child sexual abuse material, incitement to racial hatred, incitement to terrorist acts and glorification of violence, terrorism, racism and xenophobia.[501]

By analysing the above-mentioned author, the author points out that both individuals of any age group, regardless of gender, and companies regardless of the size of the company, as well as the state and its institutions, are at risk. Consequently, the scale of such attacks is incredibly broad. In Europe and globally, strategies and laws are being developed that will protect anyone in cyberspace. Therefore, it is valuable to understand the commonly accepted rules and regulations of individual countries. Consequently, the individual Baltic States will be considered below.

Cybersecurity regulations in the EU and Baltic States

It is quite difficult to imagine protecting yourself on such a large scale. And not just yourself, but your company/country. The European Union Directive (Directive (EU) 2016/1148 Of The European Parliament And The Council) seeks to ensure that each Member State of the directive can safely use cyberspace.[502] Each country follows each adaptation of this directive in order to adapt it to its citizens. An important part of the directive is devoted to

[501] European Commission (2018). Retrieved from https://ec.europa.eu/home-affairs/what-we-do/policies/organized-crime-and-human-trafficking/cybercrime_en

[502] European Parliament and Council Directive (EU) 2016/1148, 6th July 2016. *Official organ,* L 194/1

cooperation, which once again shows the importance of working together.

On February 1, 2011, the Law on Information Technologies Security in Latvia came into force. Paragraph 1 of Article 9 provides that "electronic communications companies shall ensure the integrity of the communication network in order to ensure the continuity of service provision and draw up an action plan for the continuous operation of the electronic communications network, indicating the technical and organizational measures aimed at overcoming the network and service the security threats of provision, as well as the manner in which the electronic communications merchant cooperates with the Security incident prevention institution."[503]

Paragraph 2 of Article 9 stipulates that "the Cabinet of Ministers shall determine the information to be included in the action plan for the continuous operation of the electronic communications network, the procedure for control of the implementation of this plan and the procedure for end users to temporarily close access to the electronic communications network."

As it can be found in Cybersecurity Strategy Of Latvia[504] there are following institutions (Table 1) that deal with cybersecurity problems in the territory of Latvia:

[503] Information Technology Security Law. Adopted on 28.10.2010. *Latvijas Vēstnesis*, 178/4370, 10.11.2010.

[504] Cyber Security Strategy Of Latvia 2014–2018. Retrieved from https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/lv-ncss

Table 1

Institutions that deal with cybersecurity problems in the territory of Latvia[505]

Name of the institution	Function
Ministry of Defence (MOD)	Coordinates development and implementation of information technology security and protection policy, as well as cooperates in the provision of international cooperation. The National Cybersecurity Policy Coordination Section of the MOD organises and provides support for the implementation of cybersecurity policy.
Ministry of Foreign Affairs (MFA)	Coordinates international cooperation and Latvia's participation in various international initiatives related to the cybersecurity.
Financial and Capital Market Commission FCMC)	Regulates and supervises activities in cyber space of members of the financial and capital market cyberspace; the Bank of Latvia (BoL) promotes secure and smooth operation of payment systems, while credit institutions are responsible for secure availability of electronic services in their sector.
Ministry of Economics (MoE)	Develops economic policy and promotes the development of competitiveness and innovation.
Ministry of the Interior (MoI), State Police (SP) and Security Police (SeP)	Implements the policies for combating crime, public order, security protection, and the protection of rights and legal interests of individuals, as well as coordinates the settlement of crisis situations.

[505] Author's created table according to Cyber Security Strategy Of Latvia

Name of the institution	Function
Information Technology Security Incident Response Institution CERT.LV	Monitors and analyses developments in cyber space, reacts to incidents and coordinates their prevention, carries out research, organises educational events and training, as well as supervises the implementation of obligations specified in the Law on the Security of Information Technology. CERT.LV provides support for Latvian and foreign state and municipal institutions, entrepreneurs, and individuals.
Ministry of Education and Science (MoES)	Promotes knowledge and understanding of cyber space and its secure use.
Ministry of Welfare (MoW)	Implements the social policy and the policy for the protection of children's rights.
Operation of the Safer Internet Centre of Latvia NetSafe Latvia	Is ensured by the Latvian Internet Association, educates society about possible risks and threats online, and promotes the use of secure internet content.
National Armed Forces (NAF) and Cyber Defence Unit (CDU)	Provides support in crisis situations.
Non-governmental organisations in the IT sector	Provides support, consults and cooperates with the Council in developing and implementing the cybersecurity policy.
Ministry of Transport (MoT)	Organises the implementation of communication policy.
Constitution Protection Bureau (CPB)	Oversees the critical infrastructure.

Name of the institution	Function
Ministry of Justice (MoJ) and Data State Inspectorate (DSI)	Develops, organises and coordinates the policy on rights in the field of personal data protection, freedom of information and supervision of electronic documents.
State Joint Stock Company "Latvian State Radio and Television Centre" (LSRTC)	The only provider of reliable certification services, which ensures the infrastructure of electronic identity cards and electronic signatures.
Ministry of Environmental Protection and Regional Development (MEPRD)	Organises the governance of state ICT and coordinates the electrisation of public services, whereas State Regional Development Agency (SRDA) ensures the operation and development of solutions for shared use of state ICT (Cybersecurity Strategy Of Latvia).

In the National Defence Concept clause 49 it is mentioned that to raise awareness and provide support for modern hazard situations special units are created and training in cyber defence issues is provided both in the National Guard and the Youth Guard.[506]

The author wants to point out that a lot of different institutions need to work together in order to support, consult, prevent and protect citizens from the cybercrime threats. Only having a great cooperation institution can show the best result. The next short analysis shows Lithuanian and Estonian legislation and regulation for the cybercrime.

Lithuania is also included in the states where the provisions of the Convention have become binding on its legislator, obliging it

[506] National Defence Concept. Adopted on 16.06.2016. *Latvijas Vēstnesis*, No. 117/5689, 17.06.2016.

to take all necessary measures to harmonize national legal acts with the framework set out therein.[507] The Criminal Law of the Republic of Lithuania in force is the legal act establishing liability for criminal offences known as computer crimes and Internet crimes. Sauliūnas says that the legislator of Lithuania had been combating cybercrimes since as early as 1994 by means of the amendments to the Soviet Era Criminal Code of 1961, a significant effort was required to transpose the requirements of the Convention into the Lithuanian law, starting from the year 2007.[508]

The author points out that the situation in Lithuania is very close to Latvia's – both countries are using Convention as the main document and uses different organisations to cooperate together against cybercrime.

Estonia was one of the first countries in the world to adopt a national cybersecurity strategy in 2008. The strategy was drafted by the Ministry of Defence for the period 2008–2013 and was accompanied by the Implementation Plans. The 2008 strategy offered a comprehensive view of cybersecurity and outlined the following core areas: application of a graduated system of security measures in Estonia; development of Estonia's expertise in and awareness of information security; development of an appropriate regulatory and legal framework to support the secure and seamless operability of information systems; and promoting international cooperation aimed at strengthening global cybersecurity. In September 2014, the renewed Cybersecurity Strategy for 2014–2017 was adopted, the renewal process being led by the Ministry of

[507] Global Cyber Law Database (Lithuania). Retrieved 02.05.2018. from http://www.cyberlawdb.com/gcld/lithuania/

[508] Sauliūnas, D. (2010) Legislation on cybercrime in Lithuania: development and legal gaps in comparison with the convention on cybercrime. Retrieved from https://repository.mruni.eu/handle/007/11611

Economic Affairs and Communication, with more than 30 public and private sector parties as well as academia involved in the development process.

In National Cybersecurity Organisation in Estonia it is stated that the primary cyber laws of that country are: Digital Signatures Act, Databases Act, Electronic Communications Act, Information Society Services Act, Penal Code, Code of Criminal Procedure and the Personal Data Protection Act.[509]

The author's indication is that all three Baltic States look the same at first sight, but each of them integrates European Union regulations into their vision. This is explained by the fact that each country has its own approach and its own base, which is effective.

Yet Steve Wilson, the head of the European Cybercrime Centre, noted that there were reasons to be positive about progress in tackling cybercriminals. "2016 has seen the further evolution of established cybercrime trends… However there are many positives to be taken from this year's report. Partnerships between industry and law enforcement have improved significantly, leading to the disruption or arrest of many major cyber criminal syndicates and high-profile individuals associated with child abuse, cyber intrusions and payment card fraud, and to innovative new prevention programs such as the no more ransom campaign."[510]

"For those who do not work in IT but use computing devices for work, it is necessary to have cybersecurity training so that they understand how minor mistakes or simple oversights might lead to a disastrous scenario regarding the security or bottom line of their

[509] Global Cyber Law Database (Estonia). Retrieved from http://www.cyberlawdb.com/gcld/category/europe/estonia/

[510] Ellyatt, H. (2016). The 2016 trends in cybercrime that you need to know about. Retrieved from http://www.cnbc.com/2016/09/28/the-2016-trends-in-cybercrime-that-you-need-to-know-about.html

organization,"... "With attacks becoming more advanced and sophisticated, training is mission-critical to minimize human error from the cyberattack equation."[511]

Looking at the interviews that were conducted in 2016 and 2018, the author emphasizes that cyberspace is a complex environment where security is also given a separate place. The issue of cybersecurity is definitely going to be on for years to come and cyberspace research will be a great asset.

Conclusions and recommendations

1. As it is stated in the European Council, in Europe 51 % of European citizens feel uninformed on cyber threats and 69 % of companies have no basic understanding of their exposure to cyber risks. Also the President of Latvia has told that information and understanding of cyber problems should be mentioned on the national level. That's why this topic needs to become not only a topic but also has a lot of serious consequences in different life spheres.
2. All three Baltic countries have similar cybercrime legislation but there are some differences, however, the main idea remains the same. It should be pointed out that a lot of different institutions are working together to protect country from the cybercrime threats.
3. Cybersecurity has a complex explanation that helps you understand what risks it minimizes. So in terms of cybersecurity it must be understood in cyberspace, cyber attacks and Internet in general meaning and significance. An important idea that goes through all the strategies and the European directive is cooperation,

[511] Bradford, L. (2018). What You Need To Know About Cybersecurity In 2018. Retrieved from https://www.forbes.com/sites/laurencebradford/2018/03/30/why-people-should-learn-about-cybersecurity-in-2018/#61955c4c5d00

which helps to join forces and stand up to cyber attacks. Countries need to work very closely together in this regard and realize that cybersecurity can not only be talked about in the context of a particular country.

4. It is necessary to educate internet users so that they understand how to properly use cyberspace to not endanger their data, nor themselves. This also applies to company employees and public officials, because when switching to the digital environment, not all employees understand how to deal with it and may experience problems. Therefore, it is recommended to carry out training and seminars not only for the employees joining the work, but at least once a month, because the Internet environment is changing very rapidly.

References

Bradford, L. (2018). What You Need To Know About Cybersecurity In 2018. Retrieved from https://www.forbes.com/sites/laurencebradford/2018/03/30/why-people-should-learn-about-cybersecurity-in-2018/#61955c4c5d00

Ellyatt, H. (2016). The 2016 trends in cybercrime that you need to know about. Retrieved 03.05.2018. from http://www.cnbc.com/2016/09/28/the-2016-trends-in-cybercrime-that-you-need-to-know-about.html

European Commission (2018). Retrieved 30.04.2018. from https://ec.europa.eu/home-affairs/what-we-do/policies/organized-crime-and-human-trafficking/cybercrime_en

European Council (2017). Reform of cybersecurity in Europe. Retrieved from http://www.consilium.europa.eu/en/policies/cyber-security/

European Parliament. (2018). Retrieved from http://www.europarl.europa.eu/news/en/headlines/society/20180514STO03405/pesticides-investigation-health-should-be-the-priority

Osula, A-M. (2015). National Cyber Security Organisation: Estonia. Retrieved from https://ccdcoe.org/sites/default/files/multimedia/pdf/CS_organisation_ESTONIA_032015_1.pdf

Sauliūnas, D. (2010). Legislation on cybercrime in Lithuania: development and legal gaps in comparison with the convention on cybercrime. Retrieved from https://repository.mruni.eu/handle/007/11611

European Parliament and Council Directive (EU) 2016/1148. (6th July 2016). *Official organ,* L 194/1

Information Technology Security Law. Adopted on 28.10.2010. *Latvijas Vēstnesis*, No. 178/4370, 10.11.2010.

National Defence Concept. Adopted on 16.06.2016. *Latvijas Vēstnesis*, No. 117/5689, 17.06.2016.

Cyber Security Strategy Of Latvia 2014–2018. Retrieved from https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/lv-ncss

Central Statistical Bureau of Latvia. (2018). Retrieved from http://www.csb.gov.lv/dati/statistikas-datubazes-28270.html

Cisco website. (2018). Retrieved from https://www.cisco.com/c/en/us/products/security/what-is-cybersecurity.html

Global Cyber Law Database (Estonia). Retrieved from http://www.cyberlawdb.com/gcld/category/europe/estonia/

Global Cyber Law Database (Lithuania). Retrieved from http://www.cyberlawdb.com/gcld/lithuania/

Information Technology Security Incident Response Institution of the Republic of Latvia (CERT.LV) (2012). Retrieved from https://www.cert.lv/en/

Official website of the Department of Homeland Security (2018). Cybersecurity. Retrieved from https://www.ready.gov/cybersecurity

The President of Latvia: Cybersecurity is one of our greatest challenges for the future. (2018). Retrieved from https://www.president.lv/en/news/news/the-president-of-latvia-cybersecurity-is-one-of-our-greatest-challenges-for-the-future-25408

About the Author

Elina Radionova-Girsa, *Mag.iur.*
Elina Radionova-Girsa is currently a PhD student at the Daugavpils University from 2016. She received a Master's Degree in Law at the Moscow State Industrial University. The PhD thesis is focused on cybercrime understandings and crime against a person in the cyberspace in Latvian legislation.
The author works in an e-commerce company and deals in her everyday life with fraudulent situations, cybersecurity issues and legal aspects of the companies providing services on the Internet.