Faculty of Business Studies and Law,
University „Union-Nikola Tesla” of Belgrade
Austrian Institute for European and Security Policy/AIES Wien
Institute for Corporative Security Studies, ICS, Ljubljana

CONTEMPORARY CONCEPT OF CORPORATE SECURITY

Monograph

Editor
Professor Dragan Trivan, PhD

Belgrade, 2018

CONTEMPORARY CONCEPT OF CORPORATE SECURITY

Publisher:
Faculty of Business Studies and Law, University „Union-Nikola Tesla“, Belgrade, Serbia
Austrian Institute for European and Security Policy/AIES Wien, Austria
Institute for Corporative Security Studies, ICS, Ljubljana, Slovenia

For Publisher:
dean Milan Radosavljevic, PhD, Faculty of Business Studies and Law

International Monograph of Scientific-research Interdisciplinary Project
CONTEMPORARY CONCEPT OF CORPORATE SECURITY:
No. ФП ДХ/БЕ4/0917-0618/2017-2018

Project Manager and Editor: Professor Dragan Trivan, PhD

Project funded:
Publisher: Faculty of Business Studies and Law, University „Union-Nikola Tesla“, Belgrade, Serbia
Austrian Institute for European and Security Policy/ AIES Wien, Austria
Institute for Corporative Security Studies, ICS, Ljubljana, Slovenia

Technical Editor:
Zoran Bojanić

Editorial Offices:
Faculty of Business Studies and Law in Belgrade,
11070 Belgrade, Sajmište 29, Jurija Gagarina 149A, Serbia
Website: www.fpsp.edu.rs
e-mail: info@fpsp.edu.rs

Printing
Beopress, Belgrade

Number of copies 200

ISBN 978-86-81088-12-8

Reviewers:

professor Dejan Mihailović, Monterrey Institute of Technology and Higher Education,Monterrey, Nuevo Leon, Mexico, professor Nedžad Korajlić, FCJCSS, Sarajevo BIH, professor Milan Milošević, Faculty of Business Studies and Law, Belgrade, Serbia, professor Iztok Podbregar, Faculty of Organizational Sciences in Kranj, University of Maribor, professor Polona Šprajc, Faculty of Organizational Sciences in Kranj, University of Maribor, assistant professor Slaviša Krstić, Faculty of Business Studies and Law, Belgrade, Serbia, professor Atanas Kozarev, European University, Republic of Macedonia, professor Dragomir Jovičić, Faculty „Lazar Vrkatić", Novi Sad, Serbia

Institution Associates:

Instutution Associates:
South-West University „Neofit Rilsky", Blagoevgrad, Bulgaria
„Cyril and Methodius University" Institute for Security, Defence and Peace, Skopje, Rebuplic of Macedonia
Department of Military Science, Military Academy/MoD , Skopje, Republic of Macedonia
European University, Skopje, Republic of Macedonia
Faculty of Detectives and Criminology at European University, Skopje, Republic of Macedonia
Faculty of Economies at European University, Skopje, Republic of Macedonia
Military Academy "General Mihailo Apostolski", Skopje, Republic of Macedonia
Ministry of the Interior of the Republic of Macedonia
Academy of National Security, Belgrade, Serbia
Academy of Criminalistics and Police Studies, Belgrade, Serbia
Faculty of Business Studies and Law, Belgrade, Serbia
Faculty of Law and Business Studies "dr Lazar Vrkatić", Novi Sad, Serbia
Higher School of Entrepreneurship and Security, Belgrade, Serbia
ODS EPS Distribution d.o.o, Belgrade, Serbia
Institute for Corporative Security Studies, Ljubljana, Slovenia
Criminal Justice and Security and Emergency Management, University of North Alabama, Florence, Alabama, USA

AUTHORS

Dragana Andjelković Glišović
Academy on Criminalistics and Police studies, Belgrade

Oliver Bakreski
„Cyril and Methodius" University, Skopje, Institute for Security, Defence and Peace, Skopje

Wayne P. Bergeron
Criminal Justice and Security and Emergency Management, University of North Alabama, Florence

Aleksandar Bošković
Faculty of Law and Business Studies „dr Lazar Vrkatić", Novi Sad

Filimena Bozhinovska
European University, Skopje

Milosh Bozhinovski
Ministry of the Interior of the Repablic of Macedonia, Skopje

Denis Čaleta
Institute for Corporative Security Studies, Ljubljana

Milan Daničić
Faculty of Law and Business Studies „dr Lazar Vrkatić", Novi Sad

Slavko Dubačkić
ODS EPS Distribution d.o.o, Belgrade

Dragan Ž. Đurđević
Academy of National Security, Belgrade

Božidar Forca
Faculty of Business Studies and Law of the University "Union – Nikola Tesla" in Belgrade

Tanja Kaurin
Faculty of Law and Business Studies „dr Lazar Vrkatić", Novi Sad

Elizabeta Kosteska-Miljkovic
European University, Skopje

Miodrag Komarčević
Higher School of Entrepreneurship and Security, Belgrade

Boriša Lečić
Faculty of Law and Business Studies „dr Lazar Vrkatić", Novi Sad

Boris Manov
South-West University "Neofit Rilsky", Blagoevgrad

Tanja Miloshevska
„Cyril and Methodius" University, Skopje, Institute for Security, Defence and Peace, Skopje

Toni Naumovski
Army of the Republic of Macedonia /MoD, Military Academy "General Mihailo Apostolski", Skopje

Ferdinand Odjakov
Army of the Republic of Macedonia /MoD, Military Academy "General Mihailo Apostolski", Skopje

Ljubo Pejanović
Faculty of Law and Business Studies „dr Lazar Vrkatić", Novi Sad.

Vojin Pilipović
Faculty of Law and Business Studies „dr Lazar Vrkatić“, Novi Sad

Sonja Dragović Sekulić
Faculty of Law and Business Studies „dr Lazar Vrkatić“, Novi Sad

Zdravko Skakavac
Faculty of Law and Business Studies „dr Lazar Vrkatić“, Novi Sad

Aleksandra Stankovska
Faculty of Economies at European University, Skopje

Miroslav D. Stevanović
Academy of National Security, Belgrade

Stevan Stojanović
Faculty of Business and Legal Studies, University „Union - Nikola Tesla“, Belgrade

Nenad Taneski
Department of Military Science, Military Academy “General Mihailo Apostolski”, Skopje

Miran Vršec
Institute for Corporative Security Studies, Ljubljana

CONTENT

PREFACE 13

LEGAL DETERMINATION AND PROTECTION OF A BUSINESS SECRET IN SERBIAN LEGISLATION. 17
Dragana Andjelković Glišović

INTRODUCTION 18
BUSINESS SECRET AS A LEGAL CATEGORY 21
BREACH OF BUSINESS SECRET. 24
CONFIDENTIALITY AGREEMENT. 27
CONCLUSION 30
REFERENCES 32

CORPORATIVE SECURITY IN A CONNECTED DIGITAL WORLD: LEVERAGING SOCIAL MEDIA AND EMERGING TECHNOLOGY IN CRISIS AND DISASTER 35
Wayne P. Bergeron

INTRODUCTION 36
OPPORTUNITIES AND CHALLENGES 36
SOCIAL MEDIA IN CRISIS AND DISASTER 37
SOCIAL MEDIA MANAGEMENT STRATEGY 39
THE GOOD, THE BAD, AND THE UGLY (OF SOCIAL MEDIA) 40
SOCIAL MEDIA "TRUTHS" (IF THERE IS SUCH A THING) 41
IMPLICATIONS/OUTLOOK FOR THE FUTURE 43
SOME FINAL THOUGHTS 44
SOME FINAL, FINAL THOUGHTS. 44
REFERENCES 45

SECURITY OF INFORMATION AND COMMUNICATION SYSTEMS AS PART OF CORPORATE SECURITY . . . 47
Aleksandar Bošković, Tanja Kaurin, Slavko Dubačkić

INTRODUCTION . . . 47
ENSURING BUSINESS CONTINUITY . . . 49
ANALYSIS . . . 52
SOLUTION DESIGN . . . 53
IMPLEMENTATION . . . 54
TESTING AND ACCEPTANCE . . . 55
MAINTAINANCE OF THE ACCEPTED PLAN . . . 56
INFORMATION AND COMMUNICATION SYSTEM SECURITY . . . 57
RECOMMENDED MECHANISMS FOR PROTECTION OF INFORMATION AND COMMUNICATION SYSTEMS . . . 62
IMPLEMENTATION AND IMPROVEMENT OF THE SECURITY OF INFORMATION AND COMMUNICATION SYSTEMS . . . 65
CONCLUSION . . . 67
REFERENCES . . . 70

PRIVATE AND CORPORATE SECURITY IN THE REPUBLIC OF MACEDONIA . . . 71
Filimena Bozhinovska, Milosh Bozhinovski, Elizabeta Kosteska-Miljkovic

INTRODUCTION . . . 71
THE APPEARANCE OF PRIVATE SECURITY IN THE REPUBLIC OF MACEDONIA . . . 73
DEVELOPMENT OF PRIVATE SECURITY IN THE REPUBLIC OF MACEDONIA . . 74
PRIVATE SECURITY IN OUR LEGAL SYSTEM . . . 74
DETECTIVE ACTIVITY AS PART OF THE PRIVATE SECURITY SYSTEM . . . 78
THE EXPERIENCE OF DETECTIVE ACTIVITY IN THE REPUBLIC OF MACEDONIA . . . 80
COOPERATION BETWEEN A PRIVATE DETECTIVE AND THE POLICE . . . 81
THE RELATION BETWEEN CORPORATE AND PRIVATE SECURITY . . . 82
RISK ASSESSMENT AND ASSESSMENT OF CORPORATE SAFETY . . . 84
CONCLUSION . . . 85
REFERENCES . . . 86

SOME ASPECTS OF LEGAL REGULATIONS OF CORPORATE SECURITY: AREVIEW OF THE SITUATION IN THE REPUBLIC OF SERBIA 89
Milan Danićić, Vojin Pilipović

INTRODUCTION 89
SOME ASPECTS OF GENERAL LEGAL REGULATIONS OF CORPORATIVE SECURITY..91
LEGAL REGULATION OF SOME FUNCTIONS OF CORPORATIVE SECURITY ...95
CONCLUSION 104
LITERATURE 106

CORPORATISM AS A THEORETICAL FRAMEWORK FOR THE STUDY OF CORPORATE SECURITY 109
Sonja Dragović Sekulić

INTRODUCTION 109
CONCEPTUAL DEFINITION AND DEVELOPMENT OF CORPORATISM....... 111
ITALY 114
PORTUGAL.. 116
SWITZERLAND... 117
HOLLAND... 117
BELGIUM... 117
FRANCE.. 118
CORPORATISM AND NEW WORLD ORDER................................ 119
CORPORATISM AS A FORM OF ECONOMIC SYSTEM........................ 123
CORPORATISM AS A FORM OF STATE..................................... 123
CORPORATISM AS A POLITICAL SYSTEM 124
CONCLUSION 128
REFERENCES.. 129

FOCUS OF PRIVATE HIGH EDUCATION FOR SECURITY ON CORPORATIVE SECURITY..131
Božidar Forca

INTRODUCTION 131
HIGHER EDUCATION INSTITUTIONS FOR SECURITY IN SERBIA........... 133
STUDY PROGRAMES OF EDUCATION FOR SECURITY 135
FACULTY OF DIPLOMACY AND SECURITY................................ 141
FACULTY OF INTERNATIONAL POLITICS AND SECURITY 142
FACULTY OF LAW, PUBLIC ADMINISTRATION AND SECURITY – FACULTY OF LAW 142

FACULTY OF BUSINESS STUDIES AND LAW 144
THE REASONS FOR FOCUS ON CORPORATIVE SECURITY 145
CONCLUSION 146
REFERENCES 147

CORPORATE SECURITY IN THE CYBER ENVIRONMENT 151
Tanja Kaurin, Zdravko Skakavac

INTRODUCTION 152
CYBER THREAT LANDSCAPE AND SECURITY 153
THE ELEMENTS OF CORPORATIVE SECURITY 160
MANAGEMENT OF CORPORATE SECURITY 165
CONCLUSION 170
REFERENCE 172

PLACE AND ROLE OF CORPORATE SECURITY IN THE NATIONAL SAFETY SYSTEM 175
Boriša Lečić

INTRODUCTION 176
CORPORATE SECURITY - ROLE, IMPORTANCE, PERSPECTIVE 178
COMPLEMENTARITY OF NATIONAL AND CORPORATE SECURITY 180
COMMON CHARACTERISTICS OF CORPORATE AND NATIONAL SECURITY 182
CONCLUSION 188
REFERENCES 189

POLITICAL ASPECTS OF CYBERSECURITY 193
Boris Manov

INTRODUCTION 193
THE COMMUNICATION SOCIETY 194
POLITICS AND CYBER SECURITY IN THE COMMUNICATIONS SOCIETY . . . 196
DEFINITION OF SECURITY 201
POLITICAL SECURITY IN COMMUNICATION SOCIETY. 205
CONCLUSION 211
REFERENCES 213

ORGANIZED CRIME THREATS TO CORPORATE SECURITY. 217
Tanja Miloshevska, Oliver Bakreski

INTRODUCTION 217

THE CORPORATE SECURITY ENVIRONMENT 219

THREATS TO CORPORATE SECURITY FROM ORGANIZED CRIME GROUPS . 223

BUSINESSES NEED TO ADAPT TO THE SHIFTING THREAT OF ORGANIZED CRIME 230

CONCLUSION: A COMPLEX AND MULTIFACETED WORLD 234

REFERENCES 234

CORPORATE AND SYSTEM COORDINATED INTEGRATION OF SECURITY SERVICES OF STATE AND PRIVATE SECTOR 237

Ljubo Pejanović, Stevan Stojanović, Miodrag Komarčević

INTRODUCTION 237

THEORETICAL AND METHODOLOGICAL APPROACH TO THE STUDY OF CORPORATE SECURITY 240

SYSTEM AND SECURITY SOLUTIONS OF CORPORATE INTEGRATIONS 245

CORPORATE-COORDINATED ACTIONS IN THE FIGHT AGAINST POSSIBLE THREATS. 249

CORPORATE-INTEGRATIVE ACTIVITIES WITHIN A STATE - AN EXAMPLE OF AIR TRAFFIC. 253

CONCLUSION. 254

REFERENCES 256

THE ROLE OF CORPORATE CYBER-SECURITY 259

Aleksandra Stankovska, Ferdinand Odjakov

INTRODUCTION 259

METHODOLOGY 262

ANALYSIS AND DISCUSSION. 263

CYBER SECURITY IN EUROPE 272

CYBER SECURITY IN REPUBLIC OF MACEDONIA 274

CONCLUSION 276

REFERENCE 277

THEORETICAL VIEW OF GATHERING INFORMATION FROM HUMAN SOURCES IN CORPORATE AFFAIRS 279

Miroslav D. Stevanović, Dragan Ž. Đurđević

INTRODUCTION 279

THE OBJECT AND METHOD OF INFORMATION GATHERING FROM HUMAN SOURCES. 281

THE ROLE AND GOALS OF COLLECTING DATA FROM HUMAN SOURCES . . 283

FUNCTIONS OF GATHERING INFORMATION FROM HUMAN SOURCES..... 286
THE SKILL OF GATHERING INFORMATION FROM HUMAN SOURCES 291
COLLECTING INFORMATION FROM HUMAN SOURCES IN INFORMATION AGE 294
CONCLUSION 295
REFERENCES 297

SOCIAL ENGINEERING: A BIG CORPORATIVE SECURITY CHALLENGE..301
Nenad Taneski, Toni Naumovski, Ferdinand Odjakov

INTRODUCTION 302
DEFINING SOCIAL ENGINEERING 302
MANIFESTATION OF SOCIAL ENGINEERING................................ 304
COMBATING SOCIAL ENGINEERING....................................... 310
CONCLUSION 318
REFERENCES 319

PROVIDING CORPORATE SECURITY IN CRITICAL INFRASTRUCTURE PROTECTION PROCESSES – RISK OF OUTSOURCING....................321
Miran Vršec, Denis Čaleta

INTRODUCTION 322
STARTING POINTS ON OUTSOURCING 323
INTRODUCTION OF QUALITY OUTSOURCING INTO THE CRITICAL INFRASTRUCTURE MANAGEMENT SYSTEM 325
THE ROLE OF OUTSOURCING IN INTEGRATED SECURITY SYSTEMS IN COMPANIES AND OTHER ORGANIZATIONS 331
THE MANAGEMENT OF OUTSOURCING RISKS IN CORPORATE SECURITY MANAGEMENT PROCESSES... 335
CONCLUSIONS 338
REFERENCES 339

INDEX...343

PREFACE

In the time of global interrelation and connection among national economies, security and economic development are closely related. It is unquestionable that different security risks have negative effect on the flow of people and capital, and that stable economic growth and successful management of public services encourage legitimacy and strengthen social cohesion of society, reducing the danger of its fragmentation. On the other hand, the absence of general development encourages a variety of security threats - from unemployment, poverty, political instability, to the internal and inter-state conflicts.

Modern corporations operate in a complex, and often unfavorable environment, and the current international crisis restricts their opportunities of anticipating future events and increases the uncertainty of all segments of the business. In an effort to avoid or reduce the consequences of various forms of threats to business and property, increasing attention is paid to the identification, evaluation, and risk management, thus, introducing and implementing defense mechanisms, where the biggest importance has corporate security, as an effective integrated system of internal protection of the business entity.

Theory and practice of corporate security in the Republic of Serbia and the Western Balkans are linked to the processes of extended transition, where the major research and theoretical papers on this subject are still relatively low in quantity and are from recent times. In addition, there is no agreement about the idea and content of corporate security among the theorists. However, in the former Yugoslav region the term corporate security is acknowledged today as strategic function of corporations and other business entities, aimed at business security and success in the market, through elimination of all internal and external risks and threats, minimizing risk effects, maintaining corporate operations in the time of crisis, overcoming the crisis, and resuming normal operations.

Considering the importance of social and scientific monitoring and analysis of various security aspects of current business functioning, the Faculty of business studies and law at the University "Union-Nikola Tesla", Belgrade launched international scientific-research project "Contemporary Concept of Corporate Security". The most significant result of the project is the namesake scientific monograph, whose publishers are, Faculty of business studies and law in Belgrade, Institute for corporate security studies in Ljubljana, and the Austrian Institute for European and Security Policy/AIES in Vienna. A number of authors and their editors from Serbia, Slovenia, Macedonia, Bulgaria, and the United States have participated in the creation and implementation of the monograph.

Conducted scientific project "Contemporary Concept of Corporate Security," is based on the theoretical-empirical approach, which means that certain parts of monograph have emphasized theoretical character, while a number of presented works relies on results of empirical research. The contents of scientific and professional papers of this monograph are compatible with the scientific-research project as a whole, i.e. an effort for multidisciplinary perspective and illumination of current and complex topic such is corporate security.

The results and experiences of this scientific project can encourage further research of the issues of corporate security. Also, they can be used in work on future projects at the Faculty of business studies and law in Belgrade, as well as on projects within the Ministry of education, science, and technological development of the Republic of Serbia. In addition, the monograph “Contemporary Concept of Corporate Security” could attract attention of security managers in corporations, public sector-enterprises, and specialized agencies in the field of private security, as well as interested professional public.

Belgrade, June 2018.

Project Manager and Editor
Professor Dragan Trivan, PhD

UDC 347.775(497.11)

„The open ears will not consciously keep what is entrusted to them, and the spoken word fades and will never be recalled again." **Horace**

LEGAL DETERMINATION AND PROTECTION OF A BUSINESS SECRET IN SERBIAN LEGISLATION

Dragana Andjelković Glišović
Academy on Criminalistics and Police studies

In the scientific public there is often an opinion that the issue of corporate espionage, as a very widespread weapon of modern economic warfare, is not of greater relevance. Business entities, faced with market changes, competition and customer demands, are trying to protect their ideas, information, products, since the goal of modern business is to conquer the market and achieve competitive advantage at the corporate level, that is economic domination at the global level. On the other hand, the identification of the economic potentials of the state and business systems is also dealt with by certain interest groups, foreign governments and criminal factors. By adopting the Law on Protection of Business Secrets, the need to protect business secrets was emphasized, legal certainty was achieved, and the possibility of doing business and investing funds in the research, development and supply of information that could bring economic benefits or development was achieved. In this paper, the author deals with the conceptual determination of business secrets, considering the conditions that must be met in order for some information to be treated as a business secret. Business secrets, as the right of intellectual property, include property value, not property character, based on the principle of confidentiality and the prevention of unfair competition. The possibility of filing an action for breach of business secrets has been introduced, as well as a strict criminal policy for acting in violation of the law, in the sense of responsibility for a commercial offense. On the example of a partnership between the Italian company FIAT and the Government of the Republic of Serbia, the author points to the importance of the confidentiality agreement as a successful instrument for the protection of important business data.

INTRODUCTION

In an attempt to point to complex interpersonal relationships, mistrust or human nature, secret is often viewed as a dynamic category, which at any moment can lose its significance, since Ernest Hemingway's thought is often confirmed that "*a person needs about two years to learn to talk and about 50 years to learn to keep quiet*." However, the author's intention is not to deal with secrets that are sanctioned morally, religiously or politically, but to pay attention to business subjects and the normative-legal determination of business secrets, as well as the issue of legal security in terms of its protection

Many multinational companies, faced with market changes, competition and customer demands, are trying to protect their ideas, information, products, treating them as the most valuable goods. Namely, contemporary socio-economic relations and the global way of business have imposed challenges in the national and regional economy, as well as economy at the level of economic entities. In the modern business, all possible means are applied with the aim of conquering the market and achieving competitive advantage at the corporate level, ie economic domination at the global level.

The fact that the most developed countries in the world engage national intelligence resources in the so-called market competition and careful collection of significant industrial, production or financial information about economic entities, or business competition, confirms the mutual connection between economic domination and national interest. It is clear that the goal is to enable the state or the domestic company to improve its position in the world market.

Various data and procedures treated as business secrets, although protected by internal acts of business entities, are a target of competition that also uses illegal methods for the purpose of detection and misuse. The target of theft is also information about the company itself, new products, production processes, technologies, ideas, business operations, financial reports, expert projects, marketing projects, research results, various recipes, chemical formulas, various development strategies, data on employees, help, tender information ...

Most often business secrets are given by dissatisfied employees in a competitive organization or former employees, in the hope of gaining financial gain at the expense of the former employer. Fluctuation of personnel is also a way of transmitting information on economic, economic, technological, technical and other potentials of competition, business connections and weak points of persons who participate in economic life.[1] On the other hand, the identification of the economic and economic potentials of the state and business systems is dealt with by certain interest groups, foreign governments and criminal factors.

For such activities of individuals or groups, the term economic, corporate or industrial espionage is used. There is no full consensus in the professional and scientific public regarding the determination of corporate espionage. It generally does not imply legal sources and legal information gathering, but it is also not a side-by-side method of this kind of espionage and can still be defined as a form of espionage used and implemented for commercial purposes, instead of for the purpose of national security. Namely, the scientific public recognizes two types of espionage used for commercial purposes: economic, which is characterized and implemented under the aegis of a particular state and has an international framework, and corporate or industrial spyware, which is reflected as a tool of business systems at the national level. (Aleksić, Ljubičić: 2013)

In order to avoid economic loss as a result of losing or flowing business information, it is neessary for economic entities to build their own system of information protection and determine the required level of secrecy, and in case of violation of the duty of keeping business secrets, certain legal mecha-

[1] On the world economic scene, there are numerous examples of paying damages, after losing litigation: "Volkswagen" paid General Motors a $ 100 million compensation, with the obligation to buy parts worth $ 1 billion after (in 1993) eight manager moved from "Opel" (belonging to "General Motors") to "Volkswagen", transmitting all the important business information and data they had. Famous hacker Albert Gonzales stole from the 'TJX' company access to 94 million customer credit cards due to insufficiently protected information system (he was sentenced to 40 years in prison and the company was left without clients). Former Ford engineer Xi'ang Dong Ju was arrested in 2009 and sentenced to 6 years in prison because, after 10 years in Fordu, he stole millions of dollars worth of business documentation.

nisms are available. The duty of keeping business secrets is a segment of a wider spectre of duties that are designated as such that they protect the interests of the company, even from those persons who are directly managing the company. (Milošević: 2005) On the other hand, while only persons who are legitimized as persons with special duties to a company are liable for violation of the duty of keeping business secrets, the perpetrator of the criminal offense of confiscation of business secrets can be any person.

By adopting the Law on Protection of Business Secrets, the need to protect business secrets was emphasized, legal certainty was achieved, and the possibility of doing business and investing funds in the research, development and supply of information that could bring economic benefits or development was achieved. However, it is considered that the weak point of Serbia's legal system is the fact that the definition of business secret[2] and good business practices is too wide. It is not known exactly which financial or economic data can be protected by a business secret, and it can not even be left to the full freedom of companies, for example, business secrets about the capacities, scope and structure of production from the standpoint of the balance sheet represent a state and official secret. Although the state is consciously engaged to protect a business secret, a provision by which it may come into the possession of another person, without the consent of the business secret holder, opens the possibility of abuse by persons other than its legal guardians.[3]

Business secret, as an intellectual property right, has property value, not property character, based on the principle of confidentiality and the prevention of unfair competition. The institute of unfair competition focuses primarily on the preservation of business ethics and morality and is primarily

[2] For example, the ZPD states that commercial confidentiality is an information whose communication to a third party could cause damage to the company, as well as information that has or may have economic value because it is not widely known. Such a wording suggests that there are two categories of data, where the breach of th first category causes damage to the company and the breach of the second category might bring benefit to third parties. Or, in the Law on Protection of Business Secrets, it is determined that the business secret is information that is not widely known or available to third parties. If information is not available to third parties, it should mean that it is not widely known, and vice versa.

[3] The acquisition, use or disclosure of information that represents a business secret to other persons is permitted without the consent of the holder, if it is performed in accordance with the law, or in a manner that is not in conflict with good business practices (Article 7, paragraph 2 of the Law on protection of business secrets).

concerned with the business behavior between competitors in the market. The law introduced the possibility of filing a lawsuit for violation of business secrets, as well as a strict criminal policy for acts contrary to the Law, in the sense of responsibility for a commercial offense.

BUSINESS SECRET AS A LEGAL CATEGORY

Starting from standards of ethical business, companies through the codes of business conduct promote basic values and oblige employees to act responsibly in terms of protecting confidential business information, avoiding unnecessary exposure to legal and other risks in the area of business, or causing damage to the interests of the company. It is primarily meant for any information that the company did not disclose, ie made publicly available to competitors and suppliers, such as employees' information, inventions, contracts, strategic and business plans, launch of new products, technical specifications, pricing, proposals, financial information , product costs, etc.[4]

The issue of normative regulation of the legal protection of business data and information, from various acts of unfair competition, is more comprehensively regulated by the adoption of the Law on Protection of Business Secrets (hereinafter: the Law). (Official Gazette of RS:77/2011) The previous special regulations treated the issue of business secrets in the strict sense, that is, exclusively in the domain that refers to the specific subject of legal regulation. [5] By adopting the Law, key terms and legal institutes are defined, applicable to the widest range of activities in the field of business, science and

[4] Pharmacist John Pemberton, trying to find a cure for a headache, made the most popular soft drink in the world, whose composition is still the strictest preserved business secret. Undoubtedly, "Coca-Cola" is a brand with huge competitive advantage, thanks primarily to the reputation and trust of consumers.

[5] The Law on Business Companies ("Official Gazette of the Republic of Serbia" No. 36/2011, 99/2011, 83/2014 - other Law and 5/2015, Article 72) regulates business secret in the field of business operations; The issue of the confidentiality of data submitted to the competent authority in the process of obtaining a marketing authorization is regulated by the Law on Medicinal Products and Medical Devices ("Official Gazette of RS", No. 30/2010, Article 207); The Law on Secrecy of Data ("Official Gazette of the Republic of Serbia", No. 104/2009) regulates a unique system for determining and protecting classified information of interest to national and public security, defense, internal and external affairs of the Republic of Serbia; Also, Article 50 of the Law on Trade ("Official Gazette of the Republic of Serbia" No. 53/2010) stipulates that unfair competition, among other things, is the acquisition, use and disclosure of business secrets without the consent of its holder, in order to aggravate its position on the market .

technology. It also provides conditions for sanctioning of any act of unauthorized disclosure, acquiring or using of confidential information.

A business secret, in the broadest sense, is any confidential business information that gives a natural or legal person an advantage over the competition, which has market value because it is secret and for which person that holds the secret undertakes reasonable security measures.[6] Hence, the mere fact that some information is classified as confidential does not automatically mean that it will be treated as a business secret, that is, covered by statutory protection. From the conceptual definition we set out the essential elements necessary for protection:

1) **secrecy** - is meant to be objective standards of secrecy, that is, information is not widely known and accessible to the relevant public circles, it is more precisely known only to a certain circle of persons; For example, it is possible for certain information to be communicated to other persons, without compromising its status as a business secret, however, these persons have committed themselves to certain legal means not to disclose it (by contract, legal provisions on the keeping of business secrets, etc.). [7]

2) **market value** - information has economic (commercial) value if it gives priority to its holder, that is, to the person who legally controlles it, in relation to the competition. This fact is established in each particular case by the court in the proceedings on the complaint for breach of business secrets. Since business secret is protected primarily in order to preserve the company's competitive ability, it means that they are the object of protection of information that has economic value, which provide pre-emption, as they

[6] Article 4 of the Law: Business secret, in the sense of this law, is any information that has commercial value because it is not generally known or available to third parties that could benefit economically from its use or communication, and which is by its owner protected by appropriate measures in accordance with the law, business policy, contractual obligations or appropriate standards in order to preserve its confidentiality, and whose communication to a third party could cause damage to the business secret.

[7] Professor Zabel, starting from the relativity of business secrets, believes that business secret in modern legal systems can be regarded as any information on the activity or position of an enterprise that is known, at the will of the carrier, only to a certain circle of persons in the company or outside it See: Zabel, B., Poslovna tajna, Institut za uporedno pravo, Belgrade, 1970.

contribute to the improvement or preservation of the competitive position of a particular economic entity (Zebel: 1970)

3) **"reasonable measures"** undertaken with a view to preserving its secrecy. The term "reasonable security measures" is a legal standard, and it means that concrete measures will be considered to be reasonable depending on the circumstances of each particular case, and above all on the significance and value of the information itself.[8] As a rule, the greater the value of the information, the greater the significant measures to preserve its secrecy. Some of the most common measures that are usually undertaken in order to preserve the confidentiality of confidential information are: confidential information should only be known to those persons who need it in order to be able to perform their tasks; everyone who is familiar with confidential information must be clearly informed that it is confidential or secret information; confidentiality agreements or non-disclosure of confidential information should be signed with anyone who can potentially see or receive information that is treated as a business secret, including employees, business partners, external associates, consultants; confidential documents should be labeled "confidential"; access to premises or files in which confidential information is located should be limited in the appropriate way. [9] The protection of business secrets is present as long as the information presented as a business secret is kept confidential.

All conditions must be cumulatively fulfilled, so a business secret is an information of economic value that is not widely known (it is known only to a particular circle of persons in or outside the company) and is protected by the keeper in order to preserve its secrecy.

Business secret can protect the production process, market research results, consumer profiles, financial data, business plans, suppliers and clients lists, pricing, business strategies, advertising styles, designs, drawings, ar-

[8] The measures of protection of business secrets shall be determined in accordance with the assessment of the risk of unlawful acquisition, use and disclosure of information representing business secrets (Article 5 of the Law)

[9] In legal theory there is an attitude that certain information is kept secret as a business secret also when measures are not taken, but on the basis of circumstances it can be assumed that there is an interest in keeping certain information as a business secret. See: Zabel, Ibid, p.95.

chitectural projects, building plans, and so on. Likewise, undisclosed test data also present a special type of classified information that a person who controlles them by law must reveal at the time of submission to the competent state authority for the purpose of issuing a marketing authorization for medicinal products or medical devices or agricultural chemical products using a new chemical compounds. In addition, all creative creations that are protected by intellectual property rights incorporate in themselves a business secret that has commercial value and which as such should be protected from all acts of unfair competition [10]

In theory, the question is whether a business secret can also protect the so called. negative information (eg error information to be avoided, a particular procedure that does not give the expected results, or a survey that confirms that certain ideas are useless). [11] Since any information that meets the necessary legal requirements can be treated as business secret, the opinion of the author is that this may also be negative information, having in mind their importance in preserving the company's competitive position.

BREACH OF BUSINESS SECRET

A violation of business secret is a civil law offense, but also a commercial offense and a criminal offense[12], and the degree of protection of a business

[10] According to the subjective concept, the determination of data representing a business secret, that is according to the theory of the will, holder of of business secret determined by a declaration of his will (contained in the acts of the business secret holder, such as the founding act or statute), will be considered a business secret. Objective concept, ie so-called the theory of interests, the scope of business secrets is determined, regardless of the will of the business secret holder, according to the generally recognized economic interest defined by law and other regulations. The theoretical considerations are dominated by the view that both concepts should be expressed when determining business secrets.

[11] Arsic believes that by treating such information as business secrets, it makes it impossible for a competing company to realize savings, and it is not in the general interest, since the protection of negative information as business secrets can lead to irrational spending of social assets (See: Arsić, Z., Poslovna tajna, Zbornik radova Pravnog fakulteta u Novom Sadu, No. 1/3, 1989, p. 57); Simović is of opposite oppinion, ie he believes that negative information can be a business secret (see: Simović, S., Industrijska špijunaža i zaštita poslovne tajne, doktorska teza, Kragujevac, 2012, p 191).

[12] Criminal sanctions, which in their essence represent the sharpest form of social intervention, are reserved for the most serious forms of business secrets. A prison sentence of six months to five years is confined to an unauthorized person who communicates,

secret is based on several laws. The duty of keeping business secrets is a segment of a wider confuteness of duties that are designated as such to protect the interests of the company, and even those directly managing the company. (Milošević:2005) Namely, legal responsibility, ie property and legal and labor consequences for violation of the duty of keeping a business secret is carried out by persons with special duties towards the company, or those who, due to the nature of their functions or to the extent of the given authorizations, have access to data treated with business secrets. On the other hand, while only persons who are legitimized as persons with special duties to a company are liable for violation of the duty of keeping business secrets, the perpetrator of the criminal offense of confiscation of business secrets can be any person.

The protection of a business secret lasts as long as the information representing that secret is kept confidential.[13] The author of this paper will pay special attention to the issue of unlawful acquisition, use and disclosure of information that is a business secret, regulated by the provisions of the Law on Protection of Business Secrets.

The purpose of protecting a business secret from actions of unfair competition is to legally sanction any act of unlawful disclosure and obtaining of confidential information, which is legally controlled by a natural or legal person, ie their use by third parties in a manner that is contrary to law and good business practices. Under the "method contrary to good business practices", the Law implies any action undertaken for the purpose of a market game, which inflicts or may cause damage to a competing business entity or other natural or legal person. This is particularly true for: breach of contractual provisions concerning the obligation to keep a business secret; abuse of business confidence; industrial or commercial spyware; various types of fraud; inducement to any of the above mentioned actions; the provision of data and information representing business secrets by third parties who know or were

transfers or otherwise makes available information representing business secrets or who obtains such information in the intention to hand them over to an uninvited person, provided that they are in particular confidential data, or actions taken in the interest of self-interest, is punishable by imprisonment of two to ten years and a fine, and treatment of negligence shall impose a prison sentence of up to three years. Art. 240 paragraphs 1-3. Of the Criminal Code ("Official Gazette of the Republic of Serbia", No. 85/2005, 88/2005 - cf., 107/2005 - cf., 72/2009, 111/2009, 121/2012 and 104/2013).

[13] Art. 6. Law on Protection of Business Secrets "Official Gazette of the RS ", no. 72/2011.

required to know that such information is a business secret and that it is obtained from the person in whose legal possession it is.

The Law introduced the possibility of filing a lawsuit for violation of business secrets, as well as a strict criminal policy for acting contrary to the Law, in the sense of responsibility for a commercial offense. The provisions of the Law on Protection of Business Secrets have established civil legal protection of subjects in this area in a way that in case of violation of business secrets, its holder has the possibility of filing a lawsuit (within six months from the day he learned about the violation and the perpetrator, and at the latest within three years from the date on which the violation was committed), or the initiation of proceedings before a competent court instance against any person who, through his actions, violates business secrets. This refers to the illegal acquisition, collection, disclosure, use or otherwise misuse of business secrets.

Where an offense of business secret is committed intentionally, a claim may, instead of claiming compensation for property damage, claim a threefold higher compensation than is normally determined in cases where the subject of protection is used in a lawful manner. If the obligation to keep a business secret is violated by a member of a business company, a business secret holder, in the court procedure he may request the exclusion of that person as a member of a business company, and if this is done by an employed person in a legal entity, the claim may include termination of the contract. The court may also impose a temporary measure of confiscation or exclusion from the traffic of objects containing business secrets, that is, caused by its violation, as well as the measure that prohibits the continuation of commenced operations that commit or may commit violation of business secrets.

In the event of violation of a business secret i.e. economic violation committed,[14] the foreseen fines for a company or other legal entity amount from 100,000 to 3,000,000 dinars, and for a responsible person from 50,000 to 200,000 dinars. Obligatory security measures are confiscation of goods and public announcement of the judgment.

[14] The scientific public reiterates the illogicality of legal provisions: industrial espionage is a commercial offense, and the issuance of a business secret is a criminal offense, which is unjustified, bearing in mind that there is a greater social danger of industrial espionage, and that a commercial offense is an easier offense than a criminal offense Mandić, Putnik, Milošević, Zaštita podataka i socijalni inženjering-pravni, organizacioni i bezbednosni aspekti, p. 250 and pp. 303-303.

CONFIDENTIALITY AGREEMENT

(ANĐELKOVIĆ, GLIŠOVIĆ:2016)

In the time of a developed market economy, technological revolution and great competition, every business entity strives to secure its position, preserve specific business knowledge and information, create a viable competitive advantage and impose itself on users of services by achieving good business results. In addition to evaluating and protecting its own information, it is the company's obligation to respect competition, ie not to achieve competitive advantage by using unethical and illegal practices.

Confidential information is autonomously protected by general acts, such as the statute, business secrets regulations, business regulations on the work of certain bodies, business codes, etc. An important instrument for protecting business secrets is a confidentiality agreement.[15] It is recommended that it be concluded before the commencement of negotiations, that is, in all situations where the parties have information that is protected as a business secret and are willing to exchange them under certain conditions. It contains binding terms prohibiting the other party from disclosing confidential and private information about specific knowledge, clients or products, strategic plans, and other confidential and proprietary information exclusively for a particular business entity and may be of use to competition.

For the business interests of the contracting parties not to break up or leave room for interpretation, it is necessary for the contract to precisely define which information is confidential and for what purpose they can be used. [16] If the contractual provisions are unclear or incomplete or the prosecutor

[15] It should not be mixed up with a contract on the transfer of business secrets, which allows another person, with a fee, to get acquainted with the content of information that has the status of a business secret, and consequently allows it to be used for the purpose of achieving certain business benefits. The confidentiality agreement has the object of preserving the confidentiality of the information that must be transferred to another person due to the conclusion of a particular legal transaction, according to which it is an accessory agreement; it aims to ensure the implementation of the basic contract, but by its legal nature it is independent of it See: Graić- Stepanović, S., Poslovna tajna kao predmet prava intelektualne svojine, Pravni život, No. 13/2007.

[16] What will be determined as a business secret in a specific case depends on the project itself and the business relationship, but it is important that the result of the negotiations is not too broad so that "everything is confidential", that is, business secret should include only the aspect of business that should enjoy protection and is considered confidential. It is particularly held against the authorities, as signatories of the

can not prove his claims, the court will reject the requests, making the data available to competing companies and other interested parties. The contract determines the time limit in which confidentiality of data is protected, and in business practice it is usually from one to five years, which again depends on the nature, character and significance of the protected information. As the importance of the information to be protected is complicated, the contracts are more complex, and the timeframe of duration is certainly desirable, especially if it is possible to provide for a reasonable period of protection that corresponds to the nature of the confidential information.

As due to the loss of important business information, the signed contracts get terminated or not fulfilled, violating promises, ignoring requests, allocating unnecessary financial resources and losing competitive advantage on the market, it is also recommended to include contractual dispute settlement agreements with mediation or arbitration, as well as an adequate choice of national rights to be applied in connection with a treaty in the case of international agreements. [17]

Today, the conclusion of the data confidentiality agreement is the most successful method of protecting important business data, since it is available to any private person, joint-stock company, limited liability company or other business entity. The reason why in practice there is protection of intellectual property on the basis of a confidentiality agreement is the fact that such protection has no time limit, that is, the contract can be concluded in the long run, depending on the will of the contracting parties. On the other hand, the disclosure of the secret is quite easy, especially by those who have not concluded the confidentiality agreement, and in any way came to the

confidentiality agreement, to restrict access to information by unjustifiable classification of documents with business secrets. Due to the complex administrative procedure and long deadlines, the public gets the information quite late, that is, most often, when they are no longer relevant.

[17] For the sake of this, the justification for concluding certain contracts costing our country is still doubtful: because of the “Satellite” survey from the budget reserves, Israeli company Imageset (2011) paid 27.85 million euros. The issue of disposal of natural resources was opened with the conclusion of a contract on the sale of 51% of the Petroleum Industry of Serbia to the Russian company “Gaspromneft” (2008). The two prime ministers of the two countries agreed to the sale, while the guarantees that the contractual obligations would be fulfilled were taken over by the heads of state. The issue of the controversial privatization of the Petroleum Industry of Serbia is often raised in the public domain, that is, the sale of the majority capital of this public company is characterized as a harmful business.

information. Then the holder of business secrets has no legal possibility to protect it, that is, he can not realize the compensation of damage he may have suffered. (Milosavljević:2012)

The partnership between the Italian company "FIAT Group Automobiles"[18] and the Government of the Republic of Serbia, in connection with the opening of a new factory plant in Kragujevac, was accompanied by the conclusion of a confidentiality agreement (2008), which obligated the signatories not to disclose or in any way exploit the protected information. Bearing in mind the interests of the company and its shareholders, "Fiat Group" did not publish confidential contract provisions that are key commercial and industrial secrets. In this way, the Italian partner did not want to present the business plans to the public and competition in the next ten years, with the explanation that the European Investment Bank has a complete agreement, which assessed the business venture as successful, by approving the requested loan. Representatives of "Fiat Group" also emphasized that unpublished annexes also include a business plan of the joint venture with data on the dynamics of production, which is a business secret everywhere in the world. Namely, the business plan contains data on the volume and dynamics of the production of vehicles, the markets on which they will be placed, data on the use of energy sources and a number of other technical details that can only be of interest for the competition.[19]

Although the public questioned how it is possible that a contract, concluded by the RS Government, on behalf of its people, contains a secret clause, the contract concluded to date has not been published in its entirety. Thanks to the partnership, the new factory FCA Srbija d.o.o opened in 2012, employs more than 3,000 workers and represents a desirable employer and a socially

[18] See: http://www.fiatsrbija.rs/fca/index.html

[19] The Commissioner for Information of Public Importance emphasized that the application of the right to free access to information, guaranteed by the Law on Free Access to Information of Public Importance ("Official Gazette of the Republic of Serbia" No. 120/2004, 54/2007, 104/2009 and 36 / 2010), so that the provisions of any commercial agreements can not be called into question, especially when it comes to information that is absolutely legitimate in the public interest. The provisions of the contract on joint investment of Serbia and "Fiat", which relate to the confidentiality and disclosure of information, stipulate that the obligation of confidentiality shall not be applied if the disclosure of information requires a lawful right, which is the law of the Republic of Serbia.

responsible company that strives to be a good member of the community in which it operates.[20]

CONCLUSION

In the modern business, all possible means are applied with the aim of conquering the market and achieving competitive advantage at the corporate level, ie economic domination at the global level. The fact that the most developed countries in the world engage national intelligence resources in the so-called market competition and careful collection of significant industrial, production or financial information about economic entities, or business competition, confirms the mutual connection between economic domination and national interest. It is clear that the goal is to enable the state or the domestic company to improve its position in the world market.

In the era of a developed market economy, technological revolution and great competition, every business entity tends to secure its position, preserves specific business knowledge and information, creates a sustainable competitive advantage and impose itself on users of services by achieving good business results. In addition to evaluating and protecting its own information, it is the company's obligation to respect competition, ie not to achieve competitive advantage by using unethical and illegal practices.

The issue of editing and protecting a business secret is certainly an extremely complicated and sensitive matter. In order to avoid the enormous economic damage of business entities, as a result of the loss or flow of business information, it is necessary to build their own information protection system and establish the required level of secrecy. What specific measures the holder of certain information will undertake to preserve secrecy depends primarily on the nature, significance and value of that information. The decision on business secrets must contain not only the provisions on the liability of persons who, by function, come in contact with the most reliable data, but also the obligations of all employees in the field of keeping business secrets. Establishing a business security system and permanent education of employees in the field of protection of business secrets should be one of the

[20] At the end of the current year, the signing of a ten-year contract expires, and economists warn that Fiat did not achieve the expected results in the auto industry, and call into question the extension of the contract, although in the financial statements, Fiat is the largest Serbian exporter (3% in the BDP of Serbia , and 8% in total exports).

unavoidable tasks of management of each company, and not the cost of doing business.

By adopting the Law on Protection of Business Secrets, the need to protect business secrets has been emphasized, legal certainty has been achieved, and the possibility of doing business and investing funds in research was realized, regarding development and supply of information that can bring economic benefits or development. For the first time, the general concept of business secrets is regulated, that is, elements that one information must contain to be considered a business secret, measures of protection of business secrets, as well as legal protection of business secrets from all actions of unfair competition.

However, there are objections to Serbia's legal system that claim that its definition of business secrets and good business practices is too wide. It is not known exactly which financial or economic data can be protected by a business secret, and it can not even be left to the full freedom of companies when, for example, business secrets about the capacities, scope and structure of production from the standpoint of the balance sheet represent a state and official secret. Although the state is consciously engaged to protect a business secret, a provision by which it may come into the possession of another person, without the consent of the business secret holder, opens the possibility of abuse by persons other than its legal guardians. Also, it is considered that our legal system has an insufficiently clear procedure for classification of certain information under the label "secret".

A business secret, as intellectual property right, has property value, but property character, based on the principle of confidentiality and the prevention of unfair competition.

Due to the loss of important business information, signed contracts might be terminated or they might not be fulfilled, it might violate promises, ignore requests, allocate unnecessary financial resources and lose of competitive advantage on the market. The violation of business secret is a civil-law delinquent, but also a commercial offense and a criminal offense, and the degree of protection of the business secret holder is based on several laws. Legal responsibility, ie property and legal and labor consequences for violation of the duty of keeping a business secret is borne by persons who have special duties towards the company, or which, due to the nature of their functions or to the extent of the given authorizations, have access to data treated as business secrets. On the other hand, while only persons who are legitimized as persons with special duties to a company are liable for violation of the duty of keeping business secrets, the perpetrator of the criminal offense of confiscation of business secrets can be any person.

It is particularly worrying that theft of business secrets in many private companies is not reported, as owners fear for their business reputation or simply do not want the presence of police officers inside the company.

It is clear that the desired information about economic entities can also be obtained without the use of illegal means or methods, most often through social networks. Privacy protection is one of the key problems of using the Internet. Namely, existing technologies have made it possible to collect personal data very easily and almost free of charge, and monitor the online activities of users, which is sufficient for misuse. The ability to access the Internet from public places, such as libraries or internet cafes, offers great opportunities for completely anonymous economic and intelligence work. On the other hand, it is very often emphasized that the informatics education of employees in terms of security on the Internet is quite low, which certainly poses a great danger for every company.

REFERENCES

Acin-Sigulinski S., Poslovna tajna-zalog kompanije za opstanak, Ekonomske teme, zbornik radova Ekonomskog fakulteta u Nišu, br. 2/1997.

Arsić Z., Poslovna tajna, zbornik radova Pravnog fakulteta u Novom Sadu, br. 1/3, Novi Sad 1989.

Aleksić D.; Ljubičić S., Korporativna špijunaža: normativno-kriminalistički aspekt savremenog poslovanja, Kultura polisa, god. X (2013), br. 22, str. 255-270.

Andjelković Glišović, Dragana, Milanović, Zoran, Protection of trade secrets, *Thematic Proceedings of International Significance Archibald Reiss Days* (Belgrade, 10-11 March 2016), Volume III pp. 223-237. Belgrade, Academy of Criminalistic and Police Studies, 2016.

Berle A.; Means G.,The Modern Corporation and Private Property, Transaction Publishers, Piscataway NJ 1932

Bilandžić M.,Poslovno-obavještajno djelovanje: Business intelligence u praksi, AGM, Zagreb 2008.

Bošković M.; Bošković A., „Neki aktuelni problemi od značaja za bezbednost i zaštitu korporacija", u: Naučni skup „Dani bezbjednosti" na temu: „Razvoj sistema bezbjednosti i zaštite korporacija" (Zbornik radova), Fakultet za bezbjednost i zaštitu Univerziteta Sinergija, Banja Luka 2011, str. 11–20.

Bošković M.; Keković Z., Bezbednost lica, imovine i poslovanja preduzeća, VŠUP, Beograd, 2003.

Daničić M.: Obezbeđenje lica i imovine preduzeća u Republici Srpskoj, Visoka škola unutrašnjih poslova, Banja Luka 2006.

Graić-Stepanović S., Poslovna tajna kao predmet prava intelektualne svojine, Pravni život, Beograd, br. 13/2007.

Jäger T.; Kümmel G. (eds), Private Military and Security Companies, VS Verlag für Sozialwissenschaften, Wiesbaden 2007.

Javorović B.; Bilandžić M., Poslovne informacije i business intelligence, Golden marketing & Tehnička knjiga, Zagreb 2007.

Keković Z.; Savić S.; Komazec N.; Milošević M.; Jovanović D.,Procena rizika u zaštiti lica, imovine i poslovanja, Centar za analizu rizika i upravljanje krizama, Beograd 2011.

Mandić G., Sistem obezbeđenja i zaštite,FCO, Beograd 2004.

Mandić G., Putnik N., Milošević M., Zaštita podataka i socijalni inženjering-pravni, organizacioni i bezbednosni aspekti, Fakultet bezbednosti, Beograd 2017.

Marković S., Poslovna tajna kao predmet ugovora o prenosu industrijske svojine, Pravni život, Beograd, br. 11-12/1993.

Milosavljević M., Poslovna tajna u uslugama i njena zaštita u Republici Srbiji, Pravo i usluge (zbornik radova), Kragujevac 2012.

Milošević M., „Normativna (ne)uređenost privatnog obezbeđenja lica i imovine u Republici Srbiji", u: Hadžić M. (prir.), Reforma sektora bezbednosti u Srbiji – Dostignuća i perspektive(Zbornik radova), Centar za civilno-vojne odnose, Beograd 2007, str. 127–140.

Milošević M., Poslovna tajna privrednog društva, Pravni informator, Beograd, br. 6/2005.

Milošević M., Propisi o poslovnoj tajni-pojmovno određenje i odgovornost za nepoštovanje, Izbor sudske prakse, br. 4/2007.

Nešković S., Ekonomska špijunaža I nove tehnologije u globalizovanoj medjunarodnoj zajednici, Vojno delo, br. 2/2013.

Semjonova N., Pravna pitanja zaštite poslovne tajne u Ukrajini, Pravo i privreda, Beograd, br. 9-10/2000.

Simović S., Industrijska špijunaža i zaštita poslovne tajne, Grafostil, Kragujevac 2012.

Trivan D., Korporativna bezbednost, Dosije studio, Beograd 2012.

Vukićević S., Javnost rada privrednih subjekata i poslovna tajna, Pravni život, Beograd, br. 12/2007.

Zabel B., Poslovna tajna, Servis Saveza udruženja pravnika Jugoslavije, Beograd 1970.

Zindović I.: Multinacionalne kompanije i ekonomska špijunaža, Alisa press, Kraljevo, 2008.

ZAKONI

Krivični zakonik Republike Srbije, " Službeni glasnik RS", br. 85/2005, 88/2005 - ispravka, 107/2005 - ispravka, 72/2009, 111/2009 i 121/2012.

Zakon o privrednim društvima, "Službeni glasnik RS", br. 36/2011, 99/2011 i 83/2014-dr.zakon i 5/2015.

Zakon o slobodnom pristupu informacijama od javnog značaja, "Službeni glasnik RS", br. 120/2004, 54/2007, 104/2009 i 36/2010.

Zakon o zaštiti konkurencije, "Službeni glasnik RS", br. 51/2009 i 95/2013.

Zakon o zaštiti poslovne tajne, "Službeni glasnik RS", br. 72/2011.

UDC 316.774:004

CORPORATIVE SECURITY IN A CONNECTED DIGITAL WORLD: LEVERAGING SOCIAL MEDIA AND EMERGING TECHNOLOGY IN CRISIS AND DISASTER

Dr. Wayne P. Bergeron, Lieutenant Colonel (Retired)
Assistant Professor, Criminal Justice and Security and Emergency Management, University of North Alabama, USA

We live in an ever connected and digital world which brings great convenience, capability, and comfort to our modern quality of life, but at the same time introduces significant threats and vulnerabilities as well when things fall apart or fail, as they most likely do in crisis and disaster. The purpose of this article is to provide a critical review and state of the current and future security environment related to the various areas of social media and emerging technology that impact policy, preparedness, operations, and response within crisis and disaster situations. Ultimately, we find that some of our biggest opportunities within these areas are also likewise some of the biggest potential challenges and threats we are likely to face going forward within the realm of corporative security. While we may choose to ignore these, or discount their impact in the short term, it is increasingly apparent to the enlightened observer, that they will likely manifest themselves as critical vulnerabilities and potential points of failure in the mid to long term if we do not begin to address them.

#Safety Before Selfie – Please make sure to exit the burning building before texting, tweeting, posting, or live streaming about it.

INTRODUCTION

It is a sad commentary perhaps that in our current modern society that such an emergency warning statement as the one above might actually be necessary as part of the risk communication planning of a corporative security unit, but unfortunately that is in many ways the nature of the current security and emergency management environment that exists both in the public and increasingly in the private sector as well. We currently live in an Über-connected world that allows us access to just about all the knowledge the world has ever produced at the tips of our fingers twenty-four hours a day, seven days a week, and 365 days a year in an easily accessible and on-demand format from just about any place on the face of the earth. Also, if we combine that with the potential ability to be constantly connected with the entirety of people that we have ever met or known (or desire to know) through social media and online communication platforms, it is fairly clear that we are living in a time and age that has largely never existed before and really has no real historical parallel. Of course, if you think about what we actually do with that capability on a day to day basis – the answer may not make you very proud to be a human,

OPPORTUNITIES AND CHALLENGES

As mentioned, given the current environment we potentially have an era in the field of corporative security that should allow us capabilities that far exceed anything that has ever been seen before, with a level of achievability and economic affordability that should make the most miserly, jaded, and cynical executive or manager joyous. However, as with many things, the nature of the truth is much more nuanced and the very capabilities, technologies, and break throughs that provide these advantages also potentially create or expose a set of challenges, vulnerabilities, and liabilities the likes that most of us have likely have not seen before much less have fully considered. This interplay of opportunity and challenge creates a unique security environment and ecosystem that demands a level of understanding and a comprehensive security approach that in many cases is only in its infancy in most organizations for routine operations and conditions and is likely nonexistent when it comes to crisis disaster and response situations. Hopefully, that reality begins to change, and changes quickly given the potential enormity of the consequences.

SOCIAL MEDIA IN CRISIS AND DISASTER

Whether we like it or not, social media and the digitally connected world we currently live in have in many ways changed the nature of how we as humans interact and communicate (if you are in doubt of this statement – spend half an hour with any teenager). These changes also have a profound impact on what we currently consider the necessary elements of good living and a reasonable quality of life. So much so, that in many developed countries we are beginning to see internet access and broadband connectivity being increasingly prioritized and regulated as a form of public utility akin to water and electricity versus a mere luxury commodity. Highlighting this was a recent judicial opinion in the United States that saw a judge writing in the majority opinion that "Over the past two decades, this content [internet] has transformed nearly every aspect of our lives, from profound actions like choosing a leader, building a career, and falling in love to more quotidian ones like hailing a cab and watching a movie." (Kang, 2016) Beyond the domain of individuals, we are also seeing many forward-thinking companies and organizations that are beginning to realize the value of social media technology and are "using social media tools such as wikis, blogs, microblogs and corporate social networks, they are connecting employees globally and are fostering mass collaboration. As a result, these companies are seeing improvements in communication, cross-functional collaboration and creative approaches to problem solving." (Meister and Willyerd, 2009) The end result of such innovative approaches is that these technologies and approaches are becoming a critical part, and in some cases an existential part of their business model and organizational structure. While many of these approaches are being hard-wired (so to speak) into the organizational structure and culture of these organizations, the security considerations and potential threat and vulnerability impacts are in many cases lagging behind, which creates significant hazard exposure for many organizations. In many instances, the true nature and extent of that risk is largely unknown.

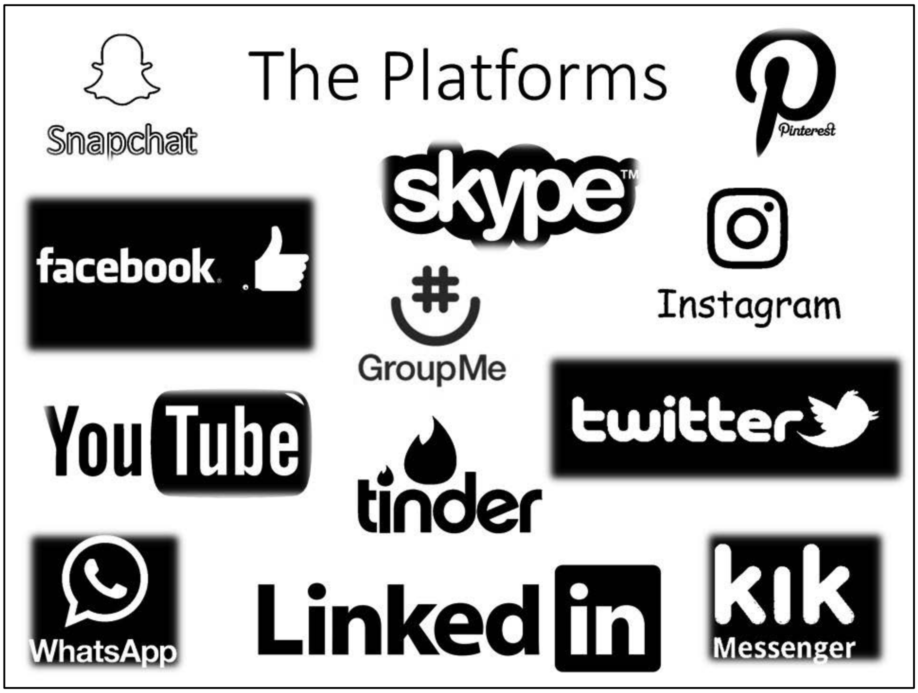


Figure 1. – The Platforms

While the individual platforms depicted in figure 1 above may change or increase or decrease in use and popularity, the nature and function of social media in today's society has largely become a constant. Regardless of the platform specifics, the fundamentals of the use of social media are largely universal and organizations, agencies and businesses need to ensure that they consider this in their crisis and disaster planning as well as every day operations both in terms of providing their core services and functions, but also in terms of security for the organization and its employees. When it comes to crisis and disaster situations, social media in many ways provides organizations a robust set of communication tools with some inherently unique capabilities that have largely been unavailable outside the realm of governments. Unlike traditional media which generally only provides one-way information dissemination, social media enables both one-way communication as well as the ability to receive feedback and communication from organizational constituents and can provide that in actual real time in most cases. Beyond just communication capabilities, when combined with aggregation, analytical tools, and data mining, the use of social media can actually become a valuable source of intelligence information and situational awareness without the need for deployment of sensors or reporting assets. In the wake of disasters, a simple capability such as the geolocation (with some limitations and caveats) can assist in actual search and rescue operations. In the case of geolocated photos, this can also provide real time rapid damage assessment capability that far exceeds traditional damage assessment methods in most cases. Additionally, beyond immediate response and recovery operations, social media platforms can provide the capability for just-in-time training for protective action procedures or video coverage and/or live streaming of events. All of these capabilities when properly integrated, can greatly enhance an organization's crisis and disaster response capability. (Bergeron, 2016)

SOCIAL MEDIA MANAGEMENT STRATEGY

However, when it comes to integrating these capabilities, the challenge for many organizations can be developing a suitable social media strategy that fits their particular organization. The key aspect that is sometimes overlooked is, that although the platforms and the technology may be new, novel, or different, at its very core a social media strategy is still really just a media management strategy and needs to adhere to the basic tenets of the organization's outcomes and objectives. Some of the key components when it comes to social media in crisis and disaster are: 1) Degraded connectivity and communications capability is a given in crisis and disaster and must be assumed and planned for up front. Graphic rich formats, embedded video, etc, that work well during normal operations will generally become an impediment to effective communication during periods of degraded and limited communication capability. Having a pre-configured plan to switch to alternate lower bandwidth, less graphical, and text-based formats should be considered and planned for up front. 2) A social media and internet communications strategy is more than just a website or Facebook page and must be comprehensive and encompass the breadth and range of platforms that constituents and customers are likely to use on a daily basis and will default to in crisis and disaster. 3) Organizational social media operations must be monitored, updated, and moderated if they have any hope of being effective. There is nothing worse than discovering months old information on a platform when searching for relevant organizational information during a crisis or disaster. 4) Organizations need to ensure they communicate on multiple platforms, to multiple audiences, utilizing multiple messages and multiple formats appropriate to both the situation and the desired outcome. 5) In terms of management and implementation, even in small organizations social media should not be considered merely an additional duty given to the newest or youngest employee. In a perfect world, the social media management strategy should garner just as much attention as other core operations functions. 6) Finally, social media messaging in crisis and disaster absolutely must be relevant and consistent across platforms and media types and be synched to organizational objectives and desired outcomes. (Bergeron, 2016)

THE GOOD, THE BAD, AND THE UGLY (OF SOCIAL MEDIA)

While for an individual it is very likely in our current “look at me” oriented world, that more comments and online attention contributes to a perception of importance, status, fame, etc.. For organizations and many high-profile individuals, more clicks, comments, “likes”, “pokes”, and shares do not necessarily equal overall effectiveness in the social media world. An organization is usually much more likely to have viral content related to lapses, mistakes, indiscretions, and bad behavior of the organization or its employees and associates as it is for outstanding performance activity. Additionally, unlike face to face interaction in most cases, the impersonal and sometimes even anonymous nature of online communications and interactions has a tendency to lead to rude and bad behavior and typically encourages the emotionalization and escalation of events that might otherwise be easily handled if conducted in person. Related to this is the fact that in some cases, “people” online may simply not be who they say they are and in some cases may not even be actual people at all in the case of “botnets” and automated response and “clickbait” server farms.

One of the incredible strengths of social media engagement for organizations can in many cases also be one of the greatest potential weaknesses and vulnerabilities as well. While a robust social media strategy and active engagement allows organizations to “speak” directly to constituents, customers, and stake holders, in crisis and disaster, many organizations will find that as the level of engagement and number of followers explodes exponentially, their capability to effectively and efficiently manage those interactions can become incredibly difficult. In such situations, the exponential "blowing up" of social media presence becomes a double-edged sword and can be particularly difficult for small and lean staffed organizations to handle. (Bergeron, 2016)

An additional challenge in the social media world is the increasing propensity for self-selection and filtering of content particularly in normal day to day and pre- crisis and disaster environments. This can also be exacerbated by the algorithmic nature of many social media network operating systems and policies, which will tend to steer their members towards similar sites such as those that they have already shown a propensity to favor. Obviously, this is not as big of a consideration in the immediate aftermath of a crisis and disaster situation as users will tend to search for the relevant content that reaches their perspective needs and is not the case with all social media platforms, additionally this can also be mitigated with multi-platform engagement. Somewhat related to the self-filtering phenomenon, is the fact that the nature of social media interaction with its inherent "trusted relationship" status between social media "friends" and connections in many cases cultivates the perfect environment for the creating, propagating and circulating conspiracy theories. In many ways social media and conspiracy theories are a perfect match and as a result, there are entire organizations, media outlets, and businesses that have been created just to debunk online, internet and social media conspiracy theories. (O'Neill, 2015)

SOCIAL MEDIA "TRUTHS" (IF THERE IS SUCH A THING)

Arguably when it comes to social media and online interaction, the nature of the truth likely changes daily, so to try and enumerate "truths" of the social media world in crisis and disaster is probably a dubious undertaking at best. However, if not immutable truths, there are at least some guiding principals and conventional wisdom that organizations should consider when operating in the social media realm, especially during times of crisis and disaster. The first factor that must be considered is that unlike traditional media sources and outlets such as radio, television, print, etc., social media is largely a "pull" medium and followers and users must specifically seek out the platforms, channels, and sites specifically. In most cases, the idea of passive exposure to social media content is highly unlikely for most organizations. One caveat to this in crisis and disaster however is the increasing tendency of traditional media outlets (especially broadcast and online) to use social media postings from organizations, agencies, and even individuals as primary sources in emerging crisis and disaster situations. This tendency provides a unique opportunity for an organization to position itself as an early authoritative source to fill the critical information void that will generally always be present in the first minutes and hours after disaster and crisis. The additional advantage here is that the organization can largely communicate directly with the public in an unfiltered manner. A note of caution on that point is in order as this capability can have unintended consequences as has been evidenced by the US White House communications staff having to scramble on a regular basis to counteract some of President Trump's most "unfiltered" Tweets. (CBS News, 2016)

As mentioned previously, one social media "truth" that is probably the most reliable and durable tenet regardless of platform, organization, or even message, is that followers will increase rapidly both during the run-up to a pending crisis or disaster as well as in its immediate aftermath. In some cases, this can be measured in thousands of new followers per hour which can seriously strain organizational resources dedicated to social media engagement activities. Clearly this is an area that should be accounted for in the organizational social media strategy and contingency planning. Of course, almost as quickly as those followers will be onboarded to social media sites and platforms during crisis and disaster, they will usually begin to separate themselves fairly soon after the immediate aftermath has passed. An innovative organization might plan to try and continue to cultivate and maintain those followers as part of its social media base.

Finally, given the unregulated and free-for-all nature of social media and the online communication environment, organizations should anticipate that they will likely be unable to fully control (or even control at all) the information environment surrounding a crisis and disaster situation. It should be assumed that there will be multiple players and they will all likely have differing agendas, motives, and desired outcomes for their engagement. Not all of them will likely be in the best interest of the impacted organization. Related to this is also the fact that criminals and scammers can and likely will also occupy the social media space and, in many cases, will compete directly with legitimate organizations and entities. (Bergeron, 2016)

IMPLICATIONS/OUTLOOK FOR THE FUTURE

When it comes to social media in crisis and disaster, it is fairly clear that the only real constant is in fact constant change. Even more so than other media environments, the social media environment is dynamic and is in a constant state of flux. Users and followers are also likewise constantly changing their likes, habits, and consumption patterns. For instance, whereas 15 years ago social media largely did not exist, and most people connected to the internet from a dialup landline phone on a desktop computer and mostly viewed static websites. Today's user and follower likely has no landline phone, connects from a mobile device through a high speed data connection, and may only communicate and interact from within a half dozen-specific applications. That means that organizations must ensure that they tailor their communications to multiple audiences, multiple mediums, and multiple messages. While doing this, it is also imperative that organizational information is planned for in an in-depth and comprehensive manner. Organizations must also remember that in most cases social media should not be relied upon or considered as a replacement for traditional media, but more as a companion or a compliment to it.

There is also another reality that goes beyond social media but is greatly enabled by it and that is the ubiquity of sensors and devices that all possess both a camera with still frame, video, and audio capture capability as well as the capability to instantly upload or broadcast that content onto social media platforms or to share it with traditional media for broadcast as well. As we have seen in many high-profile incidents, this ability has proven critical in defining and in some cases countering the narrative of agencies and organizations. Organizations and agencies must assume that every interaction of its agents and employees can and will be captured, shared, and broadcasted in crisis and disaster situations particularly when they are controversial or show the organization in a bad light. Finally, as stated previously, organizational social media strategy, policy, operations, and management simply cannot be seen as an additional duty or part time job and must be planned for well before a crisis or disaster occurs and must be carefully managed once it does.

SOME FINAL THOUGHTS

Hopefully, as we have seen based on the ideas presented previously in this article, it should be apparent that in the world of corporative security, things are always changing and evolving and when it comes to social media and emerging technology, those items tend to move faster and further than organizations do in anticipating their impact and in reacting to them. This tends to create a natural lag in the ability of organizations to keep pace and a state where organizations and entities are always trying to keep pace with a requisite set of inherent challenges and vulnerabilities as a result. Also, if we consider emerging technology and systems, organizations really need to make sure that embracing these new systems and technologies will actually benefit their mission, goals and objectives, especially when one considers that fact that many of these new additions will come with significant staffing and manpower impacts, maintenance costs, and other possible unseen mandates, liabilities, and lifecycle costs. The key is to make sure that a new capability is truly useful and enhances organizational safety, security, and effectiveness and is not embraced just because it is the newest and greatest thing and since "everyone else is doing it." It is also important to realize that in many cases the addition of a new technology or capability will also bring increased expectations on the capability of the organization which can be challenging especially in the early stages of adoption since many systems and technologies may come with a significant learning curve and a gap between initial expectations and operational capability. Care must be taken to insure that there is no lapse in organizational effectiveness in such circumstances.

SOME FINAL, FINAL THOUGHTS

Finally, given the nature of our ever connected and digital world and the fact that it brings with it great convenience, capability, and comfort to our modern quality of life, we have to remember that at the same time, social media, constant connectivity, and other emerging technologies also can introduce significant threats and vulnerabilities as well when things fall apart or fail, especially in times of crisis and disaster, as they most surely will.

This can and should have a significant impact on the state of the current and future security environment of organizations related to the various areas of social media and emerging technology. As a result, innovative and forward-thinking organizations should not merely wait or simply react to the current ever-changing technology environment, but instead should try to actively manage and shape it by ensuring that their policy, preparedness, operations, and response protocols for crisis and disaster situations are crafted with considerations of the areas previously discussed.

Ultimately, we find that some of our biggest opportunities when it comes to leveraging social media and emerging technology are also likewise some of the biggest potential challenges and threats we are likely to face going forward within the realm of corporative security, and even more so when crisis or disaster strikes. While it may be tempting at times to simply choose to ignore these or give in to the somewhat natural tendency to discount their impact in the short term, it is increasingly apparent to the enlightened observer, that when a crisis or disaster is looming or has occurred, they will likely manifest themselves as critical vulnerabilities and potential points of failure. Finally, this is true both in terms of an immediate situation but is also even more critical in the mid to long term if we do not begin to address them.

REFERENCES

Bergeron, W. (2016). Emergency Management in a Connected Digital World. Presentation at

the International Association of Emergency Managers Annual Conference, Savannah, GA. October 2016. https://iaemconference.info/2016/speakers-2/

CBS News. (2016). Aides scramble to clarify Trump's abrupt tweet about nukes. *CBS News*.

Retrieved from: https://www.cbsnews.com/news/president-elect-donald-trump-nuclear-weapons-tweet-aides-scramble-to-clarify/

Kang, C. (2016). Court Backs Rules Treating Internet as Utility, Not Luxury. *The New York*

Times. Retrieved from: https://www.nytimes.com/2016/06/15/technology/net-neutrality-fcc-appeals-court-ruling.html

Meister, J. and Willyerd, K. (2009). The Über-Connected Organization: A Mandate for 2010.

Harvard Business Review. Retrieved from: https://hbr.org/2009/11/the-uberconnected-organization

O'Neill, P. (2016). Why it's impossible to debunk a social-media conspiracy theory. *The Daily*

Dot. Retrieved from: https://www.dailydot.com/layer8/conspiracy-theories-social-media-facebook-debunking-research/

UDC 007:004.056
005.9

SECURITY OF INFORMATION AND COMMUNICATION SYSTEMS AS PART OF CORPORATE SECURITY

Aleksandar Bošković[1], Tanja Kaurin[1], Slavko Dubačkić[2]
[1]Faculty of Law and Business Studies dr Lazar Vrkatić, Novi Sad
[2]ODS EPS Distribution d.o.o, Belgrade

Effective management of a modern company is not possible without the use of an adequate information and communication infrastructure. This paper deals with the detailed elaboration of security mechanisms of information and communication systems with a special emphasis on the aspect of business continuity. Since the rapid advancement of technology over the years did not develop perfect protection, analyzes and proposed mechanisms have been developed to be applied intended for all participants in the construction and maintenance of the information and communication infrastructure of a company: from users, through system administrators to management structures. Solutions are based on the permanent and comprehensive protection of the information and communication infrastructure that can be realized through its own material and human resources, as well as the engagement of specialized companies, organizations and consultants.

INTRODUCTION

Every modern company – enterprise, corporation - increasingly relies its operations on information and communication systems. Efficient management of the company and making rational decisions is unthinkable without the use of adequate information and communication infrastructure.

Considering the constant changes in this area, the target state of the information and communication infrastructure does not represent any final situation that needs to be built. The target condition is a dynamic process that changes in line with changes in technology, environment, and other factors.

The development of a quality information and communication system should be based on the adopted standards (international, national, internal), and it is necessary to permanently perform numerous evaluations of the system and its parts. Evaluations include the evaluation of used information-communication products, intermediate products at each stage of the life cycle and end-products, i.e. installed software, hardware, network, and documentation. Observed from the point of view of complex information and communication systems in which several organizations participate in the development and implementation, the application of standards not only ensures the proper quality of the end product and the development process, but creates opportunities for the exchange of projects between individual organizations, facilitates the training of users and creates conditions for joint work on projects of representatives of different organizations.

Before the detailed elaboration of the security mechanisms of information and communication systems, the aspect of business continuity is especially emphasized. The goal of each company is to reduce the impacts that can disrupt or completely interrupt individual or all production processes. The goal is to ensure business continuity in such extraordinary situations or disasters, to maintain functional at least critical functions and to restore critical or all functions of the business within an acceptable deadline.

Prevention is probably the most important mechanism for ensuring business continuity. Throughout this paper, mechanisms have been elaborated aimed to provide smooth operation through prevention of information and communication infrastructure.

The increasing importance of information and communication technologies in business processes leads to the fact that the continuity of the business information and communication resources is extremely important for a company. The proposed analyzes and applied mechanisms are intended for all participants in the construction and maintenance of the information and communication infrastructure of a company: from the users, through the system administrator to the management structures of the company.

ENSURING BUSINESS CONTINUITY

Business continuity is a strategy that defines plans and procedures for maintaining the workings of business processes and functions, such as, for example, production, sales, finance, administration, information and communication technologies, in case of any potential interruptions in business. [ISO 22301, 2012] Unplanned business breaks can mean a loss of revenue, a reduction in reputation, a client's departure, and the like for a company or institution. Therefore, the forecasting of events and planning of recovery procedures, time constraints and other aspects are an integral part of the current business. The necessary components of business continuity planning are the estimation of losses due to a certain duration of certain undesirable events, as well as the price of establishing a normal state of critical processes.

Ensuring business continuity is an interdisciplinary concept that is used to develop a practical logistical plan for the recovery and restoration of complete or only critical functions of a company's business over a given period of time.

The relationship between the concept of business continuity and the security of information and communication systems is reflected in the fact that the security of information and communication systems refers to confidentiality, integrity and availability of information in a company or organization. [ISO / IEC 27001, 2013] Continuity of business is primarily concerned with the availability of information to those who need it. The essence of business continuity is to ensure the continuity of key business processes in a company or institution. As each business process is based on the flow of information, the focus of business continuity is on availability, that is, the preservation and recovery of vital business information.

Similarities exist in some concrete documents. For example, any methodology for business continuity prescribes the need for a risk assessment that is carried out in the same way as the assessment of the risks to the security of information and communication systems. Also, the procedure for managing incidents within the security of information and communication systems also includes response procedures in case of major damage. Therefore, a part of the documentation is also common for business continuity and security of the information system.

From the organizational point of view there are also connections. Very often, the function that takes care of business continuity is within the organizational unit that is responsible for the security of information and communication systems, although this is not always the case.

Business continuity is usually associated with large investments. When the company management reports that it is necessary to invest a lot in a backup location, which usually serves only once in ten years, then problems arise. It is therefore necessary to consider how to optimize such an investment or completely change the way of thinking.

The main purpose of a business continuity strategy is to make certain key decisions regarding the continuity of business in order to recover the business in the event of a defect in the expected time:

- how much is the target recovery time for individual business critical functions;
- what are the minimum obligations that must be carried out during the course of a disaster;
- where the backup (or some alternative) will be located;
- what resources will be needed at a backup location;
- who will be a member of crisis management;
- which is the target point for data recovery;
- what are the critical points that can cause interruption in work;
- from whom the equipment will be procured in case of damage.

Contents of the business continuity plan

Business continuity planning is an interdisciplinary activity and it includes a methodology that is used to create a practical plan describing the way a company or organization will recover and return to its original condition after partial or complete termination of critical business functions within a predetermined time after interruption or disaster.

A business continuity plan involves publication of a formal written manual that must be available for use before, during and after an interruption or disaster. Its main purpose is to reduce negative consequences for stakeholders, both in terms of type of disaster and duration. It should be borne in mind that a disaster includes all forms of economic, civil, natural, technical, secondary and consequential incidents that have a negative impact on business.

The basic part of creating a business continuity plan is determining the target time of recovery. The target recovery time represents time as well as levels in which business processes need to be re-established to avoid unwanted consequences associated with interruptions. The target time of recovery is determined at the stage of the impact analysis by the process's owners, in cooperation with those who develop the business continuity plan, and then presented to the senior management for adoption. It should be noted that the target time of recovery is the goal, not the exact value. Therefore, in practice, a strategy that will not be able to reach the target time of recovery will very often be chosen, but it nevertheless remains the goal of the next revision of the strategy. The real value in this context is called the actual recovery time, while the difference to the target time of recovery is called a "gap". The actual value of the recovery comes from simulations or exercises, or empirical, in the event of a real interruption of business.

The business continuity planning methodology should be tailored to all companies or organizations, regardless of size and complexity. Although it has roots in the industrial sector, each organization can create its business continuity plan. Statistics show that companies do not invest enough in preparing a business continuity plan, for example, a fire closes down 44% of the companies in which it occurs.

Modern business continuity plans must be flexible, they must insist on prevention, and not solely on solving already existing problems. Also, business continuity can not be viewed separately from other IT disciplines. On September 11, 2001, attacks in the United States taught a significant lesson all the business continuity planners.

Phases in the development of a business continuity plan

The business continuity plan has to be designed to be realistic and can be used in a simple way during the crisis. Therefore, it must always be available to the crisis management, along with a disaster recovery plan, and is part of the overall risk assessment of the company.

The basic phases of developing a business continuity plan are: analysis, design of solutions, implementation, testing and acceptance and maintenance of the accepted plan.

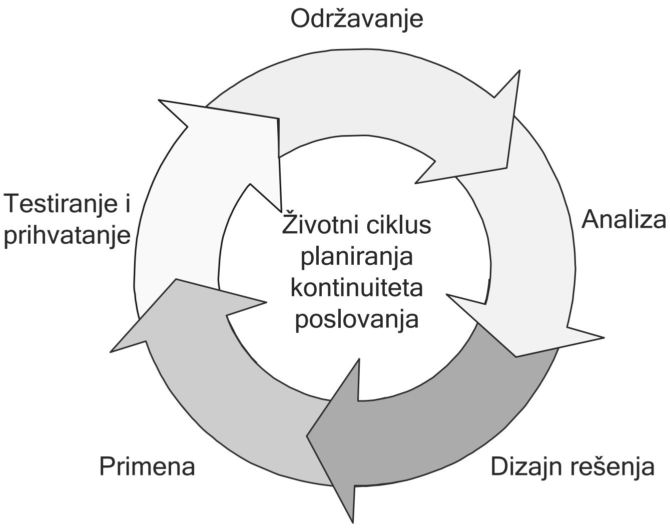


Fig. 1. Life cycle phases of a business continuity plan

održavanje – maintenance
analiza – analysis
dizajn rešenja – design solutions
životni ciklus planiranja kontinuiteta poslovanja - life cycle of continuity planning
primena-use
testiranje i prihvatanja - testing and acceptance

Analysis

The business continuity analysis phase consists of an impact analysis on business, threat analysis and the development of an impact scenario. The result of the impact analysis is the differentiation between critical and non-critical functions in the organization.

A business function is considered critical if the implications of an event occurring on an enterprise's business are unacceptable. The perception of the admissibility of the consequences of occurrence of extraordinary events may change if the cost of establishing and maintaining appropriate business or technical recovery solutions is presented. On the other hand, a certain function can be considered critical if it is defined by local legislation.

An impact analysis on business results in recovery requirements for each of the critical functions that consist of: a time limit in which a business function must be established after a disaster, business requirements for each of the functions and technical requirements that must be met in order to recover a business function.

The threat analysis follows the impact analysis. At this stage, all potential threats need to be identified in order to describe in detail the specific steps of recovery in the event of a disaster. Some common threats that are being processed at this stage are: contagious diseases, earthquakes, fire, floods, computer network attacks, corruption, power and water loss, terrorism, hurricane wind.

After defining potential threats, it is necessary to document the impact scenario. The basic rule is that planning is done for catastrophes and events of a very wide range and not for less unwanted events, as they are regularly integral parts of major catastrophes. Upon completion of the analysis phase, as its output, documented business and technical plans of requests are obtained in order to start with the implementation phase. At this stage, it is of great importance if a good asset management system is developed, since it enables easy identification of available resources. This documentation usually lists the number of required jobs at the secondary site, the persons involved in the recovery process together with the contact details and technical details, applications and data needed to function critical business functions, temporary problem avoidance solutions, deadlines allowed unavailability of business applications and more. This plan should apply to the information system as well as to all other parts of the company: general services, production, distribution or storage, and others with all their specifics.

Solution design

The aim of the design phase is to identify the financially most favorable disaster recovery solution that contains two basic requirements from the impact analysis phase: detailed threat analysis and analysis of possible impact scenarios.

At the design stage, the defined recovery requirements and recovery targets are translated operatively into concrete measures. The most important product of this phase is the establishment of a Crisis Staff Recovery Organization.

The concrete result of successful implementation of this phase is the creation of procedures for escalating, informing and activating the recovery plan itself with a focus on the critical business functions of the organization.

Usually, the organization's requirements can be expressed in the following way: minimum application and data requirements and a time limit in which minimum application and data requirements can become available again.

A disaster recovery plan may also include components outside the domain of information and communication infrastructure and applications. It may define the storage of information in paper form or define ways of re-establishing process technologies. Therefore, the business continuity planning phase overlaps with the methodology of disaster recovery planning.

The result of the design phase of the solution is a detailed description of the following functions and activities: the hierarchical structure of the crisis management, the location of the secondary workplace or building, the information and communication infrastructure between the primary and secondary workplace, the method of mapping data, applications and software that need to be operational at the secondary workplace , the physical requirements of the secondary work location.

Implementation

The implementation phase is the phase in which we implement the elements identified and defined at the design stage. It can be viewed separately from the design phase of the solution, but it continues directly on it and because of its operational character represents a significant part of the business continuity plan, both regarding cost and time.

The process of implementation and implementation of a business continuity plan can not, as a rule, be successful unless a center or a crisis headquarters for the execution of emergency actions has been established and if procedures for continuation of work, recovery and renewal are not adequately defined in the previous phases. For most organizations it is important to maintain and continually evaluate contracts with external suppliers and to maintain the reserves of all critical resources.

Finally, in the implementation phase, internal campaigns are launched on the importance of monitoring procedures related to the creation of a continuity and recovery plan and trainings, all of which are directly involved in recovery actions, as well as to all beneficiaries of the business system services. If necessary, at this stage, there is involvement of third stakeholders in the implementation of the recovery plan, such as, for example, clients, state institutions, local community.

Testing and acceptance

The purpose of the testing is to check the business continuity plan and to accept it from the company, that is to comply with all requirements that the company's management requires from the business continuity plan.

Plans may also be unsuccessful in relation to expectations due to insufficient or inaccurate anticipated recovery, design errors, or implementation of the solution. Testing can include the following stages: testing the crisis command team's call, technical transition from primary to secondary location, technical test of switching from secondary to primary location, application test, business process test, and more.

As a rule, testing is conducted at least every two years. Problems identified during the initial test phase can be transferred to the maintenance phase of the plan and can be tested again during the next test cycle. When adopting a business continuity plan, it is necessary to assess whether the introduction of measures envisaged by the business continuity plan represents an adequate response in case of identified risks.

In addition to the purely "technical" acceptability of recovery measures, they need to be in line with the goals, policies and ethical attitudes of the organization. So, for example, some recovery may be affordable for an organization, for example, moving to a secondary location that is very far away from where most of the employees live and is located in a rural, traffic-poor area, but not to employees. Some recovery measures, although very effective, eg. the "hot location" for data restoration and the re-establishment of services and services can be too expensive and therefore not acceptable to those who have a financial interest or stake in the organization's business. In the end, it often happens in practice, especially in the financial and banking sectors, that some recovery measures are acceptable to the organization for all the criteria observed, but it is not in accordance with legal regulations, that is, the legislation requires additional measures.

Therefore, when adopting measures specified in the plan, it is necessary to indicate in the measurable units what recovery measures are acceptable to all involved parties: investors, companies, legislators and clients.

Maintainance of the accepted plan

Maintaining a business continuity plan is divided into three periodic activities. The first activity is confirmation of information in the plan, distribution to all employees for insight and specific training for employees who are critical for the plan and recovery. The second activity is the testing and verification of technical solutions for the implementation of the recovery operation. The third activity is the testing and verification of documented recovery procedures, which typically occurs once a year or once every two years.

Since all companies change over time, the business continuity plan must be changed to remain relevant to the company. Typical data that need to be identified and updated within the plan are: changes in employee schedules, changes in key clients and their contact information, changes in the company's internal organization such as the opening of a new part, closing of the existing part or fundamental organizational changes.

This list of production phases is not definitive, as there are a number of factors to be considered when designing the plan itself or the manual. For example, on the matrix of risk identification, the exact definition of roles and responsibilities, where no names are listed but functions, identification of the greatest risks, strategies for their elimination, reduction or transfer, detailed plan for changing the location of resources, and more.

Due to the complexity of the approach and the requirements for a multidisciplinary approach, very often the development of business continuity plans is entrusted to independent consulting companies, although in the case of larger organizations that have well-developed information and communication support, workplace safety and general sectors, it is possible to start developing plans and manuals using their own resources and thus achieving a satisfactory level of quality of the business continuity plan.

INFORMATION AND COMMUNICATION SYSTEM SECURITY

The purpose of any serious analysis of the security of information and communication infrastructure is to point to most segments or to all segments of an information and communication system from the point of view of its safe exploitation:

- to provide an analysis of possible attacks on the system and risk analysis,
- to point out the elements that are necessary to define a security policy in order to create a secure information and communication system,
- to provide an overview of policies, processes, system structures and levels of responsibility required when building a secure information and communication system,
- to provide a detailed overview of the necessary technical guidelines and recommendations for operating systems, applications, network and communication solutions used in information and communication technologies, as well as to review procedures for several different systems and their parts.

All elements of safe and reliable exploitation of an information and communication infrastructure are intended for all participants in the construction and maintenance of an information and communication system: from users, through the system administrators to the management structures of the company. [ISO 22301, 2012]

Elements of information and communication system security

The protection of a complete information and communication system is an element that prevents the efficiency of the entire information and communication system of the company, and even other activities of the company, becoming a place for its abuse. This implies:

- normative regulation of protection by the adoption of different protection rules and
- designing and implementing technical measures for the realization of protection.

Normative regulation of the information system protection is a special area and is the subject of the activities of the state, judiciary and management and legal structures of a company.

The second aspect of the information system protection is the design and introduction of technical measures for the protection of the entire information system. [ISO 22301, 2012]

Through the development of the Internet and e-business, private computers and computer networks, if they are not adequately secured, are increasingly becoming targets of various attacks. Hackers, viruses, vindictive employees, or simple human error present clear and present hazards for the overall information systems. Also, all computer users, from ordinary Internet users to large business network users, can commit violations in terms of security of communication networks and systems.

The Internet is the largest public data transmission network that facilitates both private and business communications. The scope of business communication over the Internet is growing everyday. More and more communication is done by e-mail, there are more and more mobile or remote workers, smaller business units that use the Internet to connect to their company network, commercial transactions are done over the Internet and many other activities.

As the Internet changes and improves by offering different opportunities for business activities, the scope and type of threats, from which companies must defend themselves, also increase. Initially, these attacks were more or less harmless until they began to transmit sensitive personal or business data. In addition to losing personal or business privacy, there are also such attacks where communication resources are endangered so that they are impossible or difficult to use to any extent.

In any case, companies must be able to communicate adequately but also to defend themselves by protecting their data, resources, people, as well as data, resources and people of their partners and users.

The main attributes of security are:

- Availability ensures the survival of information and communication services, in addition to attacks aimed at endangering them. Such attacks can be triggered from anywhere. When the network is concerned, a malicious user can interfere with communication on physical channels on the physical layer and the access layer of the medium, and in the network layer, by disrupting the operation of the routing protocol, the network can break down.

- Confidentiality ensures that some information is never made available to unauthorized entities. Leakage of confidential information can have unimaginable consequences.
- Integrity guarantees that the message will never be compromised. The message can be compromised due to harmless failures, such as interference in radio transmission, or malicious attacks on the network.
- Identification allows any node to determine the identity of the node with which it is currently communicating. Without identifying, an attacker could masquerade as a legitimate node and thus gain access to information and resources, thereby affecting the work of other nodes.
- Lack of means that the sender of the message can not deny that he has sent it. Lack of denial is very important for the detection and isolation of compromised nodes. [ISO 22301, 2012]

As with any other crime, attacks on privacy and data integrity come from a small number of malicious people. In plain stealing, a thief can at one time steal one car while one hacker working at one ordinary computer can do damage to a large number of computer networks and systems. An additional problem can be the fact that most attacks on the system are made or initiated by employees within the system. Employees do damage intentionally, often from work or inaccuracies.

The part most difficult to accept is that the rapid advancement of technology that has occurred over the years,has not developed perfect protection. The answer to this question has many aspects, ranging from mistakes that are inseparable from the development of modern software, to everywhere present networking capabilities. However, basically it all comes down to something that the majority can understand: nothing earthly is perfect.

As time passes all new technologies are increasingly being developed and used to improve business and communications. At the same time, technology advances provide greater network protection capabilities. By ensuring that the company stays on top, regardless of threats and hazards, the advantages of modern communication prevail over the risks that arise.

Organization of information and communication system security

The organization of the security of the information and communication infrastructure has been implemented or should be implemented for specific processes or parts thereof which have not been implemented, through several phases that allow for systematic work. For each process, procedure, business function, the following is required:

- Define security policies and strategies.

This implies that a particular security mechanism is analyzed, examined in terms of its purposes, applicability to the real environment, analyze the necessary human and material resources, and other aspects specific to the given mechanism.

- Implement certain security mechanisms, share roles, define the structure of responsibilities.

This implies that a specific mechanism is implemented, with clearly defined roles of each individual or group in implementation.

Upon completion of the implementation, the necessary training should be made both by the user and the administrator.

- Efficient use of implemented mechanisms.

After implementation, it is necessary, in accordance with the defined roles and structure of responsibility, to apply the given mechanisms.

- Efficient use of control mechanisms to improve security.

Implemented safety mechanisms need to be systematically controlled and improved.

- Concrete technical instructions for individual segments of the system.

It involves the development of specific instructions for each participant in the system.

- Permanent system check.

Some security mechanisms need to be checked during exploitation in order to test the correctness of use.

Roles and responsibilities in the security of information and communication systems

Defining responsibilities is an integral part of each role. Each part of the system is assessed from the point of view of importance, the rules of safe behavior and the role of each individual that is assigned the competence over it.

The roles are defined from the top of a company.

Top management is responsible for defining security strategies and providing the necessary resources for the implementation of security measures.

It is also responsible for creating an appropriate climate and culture for the implementation of security measures.

Management in the area of information and communication technologies is responsible for the security of the company in the information-communication sense. It defines security mechanisms together with individuals in charge of individual business processes. It is also responsible for the correct definition of security measures and risk analysis. These persons must be fully aware of the situation in the field of security technologies.

Owners of business processes are directly responsible for the implemented defined security procedures within the scope of their competencies. They participate in security analysis, specification and classification of hazards and safety measures, development of instructions for implementation of measures. They do not participate in the immediate installation and management of security measures of information and communication systems, but participate in defining and using them.

System designers are people who participate in the development of the business system and have key roles in defining security procedures. Every business process needs to follow security policies from the beginning to the end.

Project leaders should follow the concrete implementation of security measures on the business project they lead.

Supervisors should monitor the concrete application of security measures at the level of each employee.

End users have a level of responsibility within the business processes that they perform and they have to apply security procedures within their scope of work. They need to know the basic meaning of the company's security strategy and to know their obligations in detail in this regard.

Auditors are independent persons who control and certify information and communication security. It is usually a team or a person who is not employed in the company itself, because he has a more objective view of policies, processes, security organization, and mechanisms that are used.

Classification of information in the information and communication system

The relation to information depends on their type. Different information is stored in different ways. Regarding classified information it is easier and better to develop and apply security mechanisms.

Information and data must be classified to indicate the degree of their importance in order to ensure all security attributes.

All information must have a designated owner.

The classification of information itself contributes to a greater degree of regulation of information and communication systems.

There are two basic types of information classification:

- Classification based on availability

The classification of information can be carried out on the basis of how important their availability is. In order to increase the availability of the system, preventive measures are used that aim to reduce the likelihood of system failure and also measures to restore the system to reduce system failure time.

- Sensitivity classification

Classification of data / process based on sensitivity can be done by their division into security classes. [ISO / IEC 27001, 2013]

RECOMMENDED MECHANISMS FOR PROTECTION OF INFORMATION AND COMMUNICATION SYSTEMS

There are many concrete mechanisms that are used or could be used in the information and communication infrastructure in order to ensure its security. Some are listed here, although it is a segment of information and communication technology that changes rapidly.

It should also be noted that each of the above mechanisms (and those not mentioned herein) should be thoroughly analyzed and applied.

- Control of access to information
- Identification, authorization and control mechanisms refer to identification, authorization and control when linking users to a network resource. Often, these mechanisms are called the “big three” of the management and administration of computer networks.
- Access lists define the access rights to an object. Usually, they are defined on access network routers, central network routers, proxy servers,

identification, authorization and control servers, domain controllers, and other devices and servers. [Kalsi, 2016]

- Software security

General requirements are related to the following:

- separate the development and production environment and data,
- consider the possibility of system security being embedded in software development,
- check that the data have confidential information and if they do treat them accordingly,
- use proven development tools and software,
- require that the software also delivers instructions for use, for installation, for administration, and for safety. [Meier, 2011]

- Monitoring

Continuous monitoring - Monitoring activities on the information and communication infrastructure is necessary for quality maintenance and improvement of the same. [Kalsi, 2016]

- Cryptography

Three types of cryptography are analyzed and applied: cryptography of wide area network connections, digital signature and digital certificate, and protection against unauthorized access to devices. [Duggan, 2014]

- Anti-virus protection

The need for protection against viruses is evident already in home computers connected to the Internet, while in the case of a computer network, the importance of the data that can be lost and the material damage that potentially failing the system causes is absolute necessity. [Kalsi, 2016]

- Backing up data and loading them

Backing up data is an operation by which all significant data, including software and network device configurations, are copied from the information system device - computer, server, network device - to a large capacity device, so that data can be restored if and the information system is restored from these stored data. [Preston, 2006]

- Local Area Network / Wide Area Network

Network security is one of the most important segments of the security of an information system, and therefore the entire company.

In the analysis of the network environment, it is important to define a perimeter - the virtual boundary between the local and the public network. Many protection mechanisms are implemented on the perimeter.

The following are the segments that are specially analyzed:

- Local information and communication infrastructure (network equipment, generic cable system, system servers / services);
- Network security mechanisms (firewall, demilitarized zones, detection and intrusion prevention systems, virtual private networks, redundant connections, redundancy of network components, etc.);
- Monitoring and managing networks (network monitoring and access control). [Duggan, 2014]
- Redundancy

Redundancy increases the availability of the system and can be implemented at the application / service level (application and system software), hardware level (computer and communication equipment) or on the communication links themselves. [Duggan, 2014]

- Equipment accommodation conditions

Conditions for accommodation of equipment must be adequate. This is especially true for server rooms and rooms for the accommodation of communication equipment. In addition to providing air-conditioned environment, the segment of access control is very important, as well as video surveillance, overvoltage protection, power supply and the like [ISO/IEC 11801, 2010]

- Physical technical safety

In addition to the protection that relates to elements of physical and technical protection of the facilities, the information and communication infrastructure has additional requirements:

- Technical protection (protection of access to devices, fire protection, water protection);
- Surge protection (protection against electrical network problems, protection against atmospheric discharges);
- Security of removable media. [Vaca, 2001]

IMPLEMENTATION AND IMPROVEMENT OF THE SECURITY OF INFORMATION AND COMMUNICATION SYSTEMS

Modern trends in the development of information and communication systems and services point to the need for permanent modernization of all aspects of security. New devices are emerging, new communication mechanisms, accessibility of certain technological solutions (economically acceptable price, etc.) increases. It also increases the requirements of the users for different types of services that can be implemented on the information and communication infrastructure as well as on the capacities of individual services (a larger number of users, higher requirements for bandwidths and speeds, and more).

With the development of new technologies there are new opportunities for improving business and communication. At the same time, the advancement of technology provides greater opportunities for attack but also for the protection of such business and communications.

The preceding chapters only list various types of possible hazards and attacks on the information system as well as the mechanisms and procedures of defense against such attacks. We do not think that we have managed to capture all possible cases of either attack or defense. We tried to point out the most common and most effective of them. New ways of better communication are emerging continuously. At the same time, the methods of attack against it, as well as the mechanisms of defense, are being developed.

According to official data, the use of the Internet continues to grow. Not only by the number of users but also by the type and scope of services that are offered. These large numbers speak of a very wide area for business as well as for criminal activities. The game of chasing the perpetrators of criminal activities in this ambient is infinite. There are more and more examples in the world and in our country.

The development of information and communication systems, as a basic element of modern business, is the basis for reliable, safe and successful communication. The right attitude towards business-to-enterprise information and the creation of a system that conforms to global standards are the goals to strive for.

The first step is to look at real needs and a resolve to have implementation. In particular, this refers to the improvement of information and communication infrastructure and the development of security mechanisms. This implies normative regulation of the protection of information and communication systems by adopting various formal decisions and rules on protection of the information system. One of the recommended ways to implement this segment is the decision to introduce the ISO 27001 security standard. In this part, there is a special responsibility on the management and legal structures of the company.

The next step is implementation. It involves a comprehensive assessment and audit of systems, information and business. This requires certain investments in material resources and in people. Material costs are relatively easy to estimate. The necessary investments in people are harder measurable and significant.

The third step is the exploitation, maintenance and improvement of the entire information and communication infrastructure. This step involves permanent implementation of defined procedures and actions for the purpose of maintenance and development of information and communication systems. In accordance with the development of information and communication technologies, there is a need for continuous control and improvement of the system. Here we especially emphasize the need for professional training of those responsible for this step in the maintenance and development of information and communication systems.

Particular attention in the exploitation, maintenance and improvement of information and communication infrastructure is the safety of the system. By ensuring that the company stays on top, regardless of threats and hazards, the advantages of modern communication prevail over the risks that arise. The process of introducing protection is an enormous and important work.

With the rapid advancement of technology over the years, “perfect protection” has not been developed. There is no way for anyone to be absolutely safe. The answer to this question has many aspects ranging from faults that are inseparable from the development of modern software to ever present possible network connectivity. However, basically it all comes down to something that the majority can understand: nothing earthly is perfect.

The solution is in the permanent and comprehensive protection of the information and communication infrastructure that can be realized through our own material and human resources, as well as the engagement of specialized companies, organizations and consultants.

CONCLUSION

In information and communication technologies it is difficult to predict what will happen in the future and how quickly changes will happen. It is possible to talk about currently applicable concepts and mechanisms. Nevertheless, certain predictions, at least at the conceptual level, must be made. One of these predictions is the development of information solutions in the so-called. service-oriented architecture. [Sweeney, 2010] Here, only the basic concepts of this architecture and the position of information and communication infrastructure within this concept are mentioned, because, according to the author of this document, that is a trend in which a modern information and communication infrastructure should be developed.

In information and communication technologies, service-oriented architecture is a set of concepts that are used in the development of information and communication infrastructure and its integration with the goal of full functionality and interoperability of implemented services. In these solutions, individual services can be developed and implemented by different manufacturers, but they must be provided with mutual integration for data exchange and process control.

The service orientation principle calls for the independence of the service from the operating system and other information-communication technologies that function in the background. The focus is on firm connections between business processes and information-communication architecture.

Typical service features of service-oriented architectures are:

- the connection between system components through defined interfaces, internal functions, structures and states of individual components are completely internal and do not affect the work of other components in the system,
- interconnection of individual components is done as needed, it is possible to harmonize components with defined rules of a particular service (functionality, interfaces, inputs and outputs).

The basic precondition for the development of a service orientation is the decomposition of functional processes into modular units - services or subprocesses that, with the help of information systems, provide optimum support for one or more business processes.

Solutions with service-oriented architecture naturally rely on the information and communication infrastructure in their implementation. The network allows the various elements of the system to interact with each other by providing a connection between them. Of course, the network also provides more than that. In any case, the network is there to enable applications with a service-oriented architecture to focus on their underlying issues.

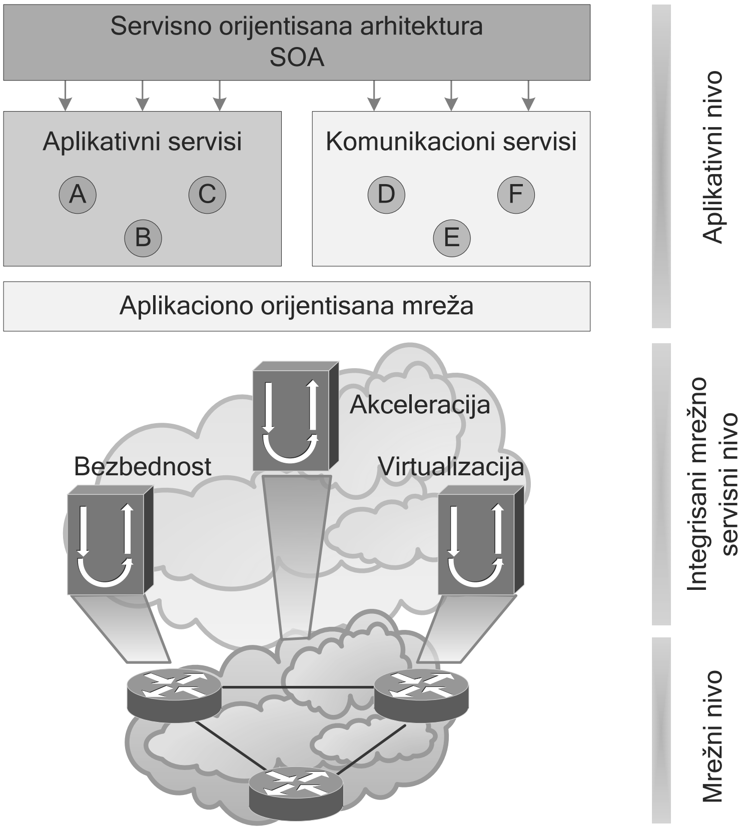


Fig. 2 Information and communication infrastructure in a service-oriented network architecture

servisno orijentisana arhitektura – service-oriented architecture SOA
aplikativni servisi – application service

kominikacioni servisi – communication service
aplikaciono orijentisana mreža –application oriented network
bezbednost-security
akceleracija-acceleration
vizualizacija-visualization
mrežni nivo – network level
integrisani mrežno servisni nivo - integrated network service level
aplikativni nivo-application level

Figure 2 presents the main elements of one such architecture:

- Base Network Level - Network availability and service quality are critical parameters for supporting service-oriented architecture solutions.
- Optimization, virtualization, security - Application Service with Service-Oriented Architecture provide their maxims in scalable and secure performance environments.
- Application level - Applications with service-oriented architecture represent a combination of traditional concepts of business applications and communication and application services.

Without network service-oriented architecture can not function because all communication between these application solutions takes place over the network. But the network does much more. At the network level, many other parameters are set up: access rights, bandwidth, data transfer control, security and everything else that has a significant impact on the operation of applications with service-oriented architecture. For example, links in a wide area network have a significant impact on the performance of applications with service-oriented architecture and all other applications.

As far as information and communication infrastructure is concerned, the goal is to build a service-oriented network architecture, [Ganapathy, 2008], which will also include network and integrated network service level from the previous scheme.

A further step would be to build a secure service-oriented network architecture. The designed information and communication infrastructure enables applications with service-oriented architecture to function fully, securely and reliably, and consequently, business processes that use applications with service-oriented architecture are improved and optimized with the ultimate goal of better business.

REFERENCES

Duggan, M. J., (2014). *Cisco CCIE Routing and Switching v5.0 Configuration Practice Labs*, Cisco Press, Indianapolis.

Ganapathy, S., (2008). *Implementation of a Service-oriented Network Architecture,* University of Massachusetts, Amherst

ISO 22301, (2012). *Societal security – Business continuity management systems – Requirements*, International Organization for Standardization.

ISO/IEC 11801, (2010). *Information technology – Generic cabling for customer premises*, International Organization for Standardization.

ISO/IEC 27001, (2013). *Information technology – Security techniques – Information security management systems – Requirements*, International Organization for Standardization.

Kalsi, B. S., (2016). *IC3 Certification Guide Using Microsoft Windows 10 & Microsoft Office 2016*, Cengage Learning, Boston.

Meier, J. D., (2011). *Improving Web Application Security – Threats and Countermeasures*, Microsoft Press.

Preston, W. C., (2006). *Backup and Recovery*, O´Reilly Media Inc, Sebastopol.

Sweeney, R., (2010). *Achieving Service-Oriented Architecture: Applying an Enterprise Architecture Approach,* John Wiley & Sons Inc., New Jersey

Vacca, J. R., (2001). *The Cabling Handbook*, Prentice Hall PTR, New Jersey.

UDC 334.728:351.759.4/.5(497.7)

PRIVATE AND CORPORATE SECURITY IN THE REPUBLIC OF MACEDONIA

M-r Filimena Bozhinovska[1], Milosh Bozhinovski [2], Elizabeta Kosteska-Miljkovic[3]

Private security is increasingly becoming a socially important industry. If we take into account the risks of modern life, private security appears as an indispensable aspect of society. Questions about corporate security systems are certainly among the most difficult issues, so in this paper we will make a distinction between private and corporate security as well as their interpersonal relationship. The protection of the assets of the corporation must be a priority for the company's corporate security, which must be exceptionally well organized, bearing in mind the motives of the owners of the property and the capital to protect them at all costs.

INTRODUCTION

Private security is a new term in the Macedonian language security lexicon, which appears together with the need to protect private property, with the emphasis on defining the main focus on the individualisation of security, and thus by defining the specific risks and laws that exist in relation to individuals and / or groups. Security as a term is most often used on the uniforms of persons who perform the role of protection of property and persons, whereby we can say that it is taken from the western global trends that uncontrollably penetrate the mass media in our country. Asset and property

[1] *Criminalistics assistant, European University-Republic of Macedonia*

[2] *Graduate Detective Independent Inspector of the MUP of the Republic of Macedonia*

[3] *Master student of national security, European University-Republic of Macedonia*

security agencies are legal entities that perform service activities to protect the private property of individuals. Detective agencies, or private detectives, represent the second segment that takes care of private property protection and represents the service activity of physical and legal persons in order to improve their security and fulfill certain needs, while privacy is guaranteed by strict discretion. The difference between the agencies for the security of persons and property and the detective agencies consists of legal authorizations, whereby persons in the agencies for securing property and persons who conducts physical and technical protection - the security of property and persons, and private detectives carry out the collection of adequate knowledge for the preventive action against possible risks and threats to private property (William and Todd, 1984). Further in this paper, we will look at the notion of private security, detective activities and cooperation with the police. Special emphasis should be placed on corporate security aimed at detecting fraud and misconduct, and examining and making cases of corporate crises, crime, and other criminal offenses that corporate security professionals should be aware of in order to ensure effective protection of people, operations, and funds. The existence of an effective corporate security system protects the company from all forms of threats, establishes the basis for making management decisions, provides top management access to classified information, and forms processes and procedures that prevent the release of protected data from the corporation (Bakreski, Trivan and Mitevski, 2014). The Republic of Macedonia is a country with a managerial deficit in the field of corporate security, which is an important signpost for the importance of corporate security, as well as the need for the same for companies and firms in the Republic of Macedonia. The applicative character and basic aim of this paper is to give a clearer picture of the significance and needs of corporate security in companies in the Republic of Macedonia, as well as the role of the state security system in the fight against all risks and unwanted factors that can arise during the operation and functioning of companies in the Republic of Macedonia.

THE APPEARANCE OF PRIVATE SECURITY IN THE REPUBLIC OF MACEDONIA

With the transformation of public capital in Macedonia from state to private, there was also a growing need for protection and securing private property (Slaveski, 2009). According to Grozdan Cvetkovski, the conceptualization of private security in Macedonia took place in three directions. Namely, he makes a distinction between the sphere of jurisdiction between detective activity, security activities and technical protection, as three sub-systems of the private security sector. The answer to the question of why for a long time these three segments of private security did not exist in normative regulation, apart from the problems with a legal vacuum that was objective in nature because the previous value criteria had been abandoned and the new one was hardly created, he asked for subjective reasons and the lack of democracy in the first years after gaining independence of Macedonia (Cvetkovski, 2014). In this period, the security agencies gained importance after the adoption of the Constitution in 1991, when ownership rights were granted a constitutional category, while at the same time the category of social ownership was abolished (Bakreski and Milosevik, 2010). Since 1991, until 1999, this matter had not been regulated by law. For nine years, the security agencies practically worked illegally, and this was possible primarily because their owners were either high-ranking police officers or their closest relatives.

The legal basis for the establishment of entities that will be engaged in private security activities was established by the Law on Detective Activity and the Law on Security of Persons and Property of 1999 (Law 80/99), as well as the Law on Procurement, Possession and Carrying of Weapons from 2005 (Law 07/05). After more than a decade of experience, in 2012 an entirely new Law on Private Security was adopted, which made additional steps to regulate numerous problems that have arisen in this sphere. In this short period since the beginning of the work of the private security sector in the Republic of Macedonia, we can distinguish several problems that have arisen from its functioning. In relation to asset protection agencies and persons, or as defined by the new law as "legal persons with a private security license", there were no adequate standards and professional ethics in the work of this sector. The new Law on Private Security makes an effort to tighten the conditions for the operation of these non-partisan security actors, but practice shows that we are still far from European standards in this area. What has been missing in the past is improving communication between the state and the private security sector, which needs to be improved because both sectors are intended to protect the public interest, that is, to contribute to the prevention and reduction of crime rates in the country. Above all, it is most important to find mechanisms to improve supervision of these private security actors, both by the government and parliament, and by the civil society.

DEVELOPMENT OF PRIVATE SECURITY IN THE REPUBLIC OF MACEDONIA

Together with the transformation of social capital in the Republic of Macedonia (RM) from public to private, there was also a growing need for protection and securing of private property. In the society itself, the prevailing awareness that the effective regulatory system for private security services is an important element for increasing the contribution of this sector in relation to crime prevention and citizens' security, is prevalent.

Cooperation with the Ministry of Internal Affairs focuses on the organization of seminars and other workshops for the work of this profession, as well as the development of manuals on specific issues, such as the Manual for civil servants for the enforcement of laws on the role and accountability of the police in conducting control and supervision of private companies security

In practice, contracts are obtained through public tenders where they select companies that offer the lowest price for providing private security services. Price for security services is 2.2. Euro (for physical security, according to the Informal Act of the Chamber) The impact of the economic crisis is still present with every business aspect, especially in the service market.

PRIVATE SECURITY IN OUR LEGAL SYSTEM

From the legislative point of view, corporate security in our legal system is regulated by the Law on Private Security (Law 12/2012), with amendments (Laws 164/13 and 193/2015). This Law regulates questions about the manner and conditions of private security, as authorized by employees who perform private security. Private security is a matter of public interest, and it is carried out by legal entities that have a private security license issued by the

Minister of Internal Affairs in the prescribed procedure, after fulfillment of certain legal requirements. Private security is the protection of persons and property carried out by legal persons having a private security license. In the performance of security, they must not use operational methods and resources, for which the application of the law is authorized by the competent state authorities (primarily to the police, the financial police and other competent authorities). Likewise, they must not provide security for persons and property that, on the basis of special regulations, are provided by the competent state authorities. Private security is performed: in the form of providing services and for own needs. Private security in the form of service provision is performed as: physical security and technical security, while for its own needs it is performed as a physical security, as a physical protection and monitoring security.

Legal entities that carry out private security activities join together into the Chamber of the Republic of Macedonia, and in this Chamber, it is possible to bring together legal entities that perform private security for their own needs. Legal persons having a private security license have the authority to take measures and activities in order to prevent and detect harmful occurrences and unlawful acts that endanger the physical integrity and dignity of the persons and property that they protect (Bakreski et al., 2012). Legal entities that carry out private security services must not provide persons and property that, on the basis of special regulations, are provided by the competent state bodies, nor perform duties related to collection of debts. Supervision over the implementation of this law, as well as the regulations adopted on the basis thereof, is carried out by the authorized officials of the Ministry of Internal Affairs.

Private security, under conditions determined by law, shall be executed:
A) in the form of service provision and,
B) for their own needs.

A) Private security in the form of service provision is executed as:
- Physical and technical security

Physical security can be performed by using firearms, especially for the security of: persons provided with physical protection, legal persons handling money and other valuable items, transportation and transfer of money and valuables, and facilities and property they protect. A security worker (a person who owns a license and who has a working relationship in a legal entity that carries out private security) can use only firearms owned by a legal person for private security (physical weapons are supplied in accordance with the regulations on weapons). These persons can carry weapons and ammunition only in the facilities they provide, or within the boundaries of the security area. Physical protection of persons and property is done directly by security personnel. When monitoring-patrol security is performed, a security and surveillance center is established. It is a specially secured room equipped with technical devices and devices for receiving alarm signals. A legal entity that performs private security in the form of service provision can provide security by transferring and transporting money or other valuable items with a specially equipped vehicle and without a specially equipped vehicle, if it has a safety suitcase. Similarly, private security in the form of service provision can be used to maintain public order at public gatherings, sports events, cultural, entertainment, religious, political and other events. This type of security is done by wearing a special type of clothes and without the carrying of a firearm. Technical security is provided by the use of technical means and devices in order to prevent unlawful actions directed at persons and property being protected. Technical security is especially useful in these cases: detection of unauthorized access to buildings and premises; the prevention of unauthorized entry of firearms, explosive, radioactive, toxic substances; in attacks on security workers or money transport vehicles; unauthorized access to data and documentation. Technical security is especially performed by technical teams and video surveillance equipment, whereby it is necessary to place a notice on it in a visible place.

B) Security for their own needs

A legal entity may obtain a security clearance for its own needs for the protection of its property and its persons. This security is provided by persons employed in a legal entity whose assets and employees are provided. This legal entity may not provide private security services to other natural or legal persons. The Law on Private Security, for legal entities whose activity is connected with the handling of radioactive and other dangerous substances, as well as cases of special cultural and historical significance, or it is about the defense and security of the country, it is prescribed that they must have private security (the same can be for own needs or by using services from legal entities that perform private security).

C) Authority of security workers

In the performing of their statutory powers, security employees are obliged to respect the basic human freedoms and rights and dignity of citizens. The application of their powers must be proportionate to the need for which they apply the same, and of course it is necessary that greater property damage is not caused by the authorized action. During the performance of private security, the security worker:

- Can verify the identity of the person at the entrance and exit from the property / space that is provided or is caught in the commission of a criminal offense, or upon the order of an official person of the Ministry of Interior;
- Warns persons to distance themselves from the property / space they provide, or does not allow the entry of uninvited / unauthorized persons, and may prohibit unauthorized recording;
- He may retain the person in the execution of a criminal offense which is prosecuted in an official capacity and immediately informs the police about this;
- Performs a review of persons, objects, vehicles, luggage, at the entrance and exit to the space / property being provided.
- When performing security, the security worker can also use the means of coercion: physical force, rubber rod, binding of persons, chemicals (spray), firearms.

The use of these means must be proportionate to resistance and subsidiary (in the event that the aim can be achieved through a milder action,, then no greater use of coercion is used). A security officer may use firearms only if he is objectively unable to notify the police and, if he otherwise can not stop a simultaneous unlawful attack on his life or a person that he protects (a necessary defense) and can not stop an immediate attack on the property he protects. An attack is understood to mean any physical attack in a way or by means of an immediate threat to life, an attack carried out by two or more persons, an attack by a clearly stronger person who uses special skills. The law has defined that the term “property attack” is any act aimed at the destruction, deterioration or alienation of the property being secured. Legal restrictions on the use of firearms are also prescribed. The security guard first alerts the person clearly about his intention. The use of firearms is prohibited if it puts the lives of other citizens at risk, if it is against a child, an elderly or pregnant woman, except in the case when those persons used firearms.

For each person's detention, as well as the use of coercive means, the security worker is obliged to compile a written report to the MIA. After briefly outlining the site and the manner of performing private security in our legal system, it follows that private security providers have the legal right to use coercive means, which include the use of firearms.

DETECTIVE ACTIVITY AS PART OF THE PRIVATE SECURITY SYSTEM

Private detective activity, in general, has a very long history of development. In the second half of the twentieth century, in the United States, and somewhat to a lesser extent in Europe, there was an accelerated dynamic in the development of this activity. In the countries that emerged after the collapse of the Eastern Bloc, this activity began with its development over the past two decades, in parallel with the transition process, and in this context with the privatization of certain sectors of the security system. As a relatively new profession in these countries, it had not always been sufficiently explored, both in theory and in practical terms. The number of authors and papers dealing with this issue is still insufficient (Cvetkovski, 2011), unlike the developed western states where this topic is being treated since the end of the 1980s. Because of the fact that as clients of detective services, besides citizens, there are also law offices, and often state institutions and governments, they need to take a more complete view of the current position, development and prospects of this activity in post-communist countries.

Private detective activity, as a global phenomenon from the end of the last and the beginning of this century, has experienced significant expansion in development over the past two decades, and especially as a know-how profession in the post-communist and transition countries (Cvetkovski, 2014). In this regard, and starting from international practice globally, it is important to point out that the US economic system, as the most liberal, first recognized the need of an individual for a greater degree of individual security services than those which the state provides standardly, which is why they started using the services of private security agencies. Detectives and investigators occupy about 52,000 jobs in the US private security industry (Dempsey, 2011). About one third of them belong to the category of self-employed persons, including a large number of persons with whom it is a secondary profession, as self-employed private detectives. Approximately one-fifth of these jobs are deployed in research and security services, including private security agencies, while the rest are working in companies from the domain of securing trade companies or in commodity houses and other large stores. The remaining jobs fall primarily on the state and local self-government; legal services firms; companies that provide employment services; insurance companies; the banking sector and other sectors which deal with deposits.

For these working positions, competition is extremely high because it attracts a large number of highly qualified people, including relatively young pensioners from law-enforcement institutions, as well as persons with previous military careers. Employment opportunities in this sector are limited at different levels, that is, they can only be reached through the detective agencies or agencies for engaging part-time detectives. Increased demand in relation to private detectives and investigations is a result of fear of crime, increased number of court proceedings, and the need to protect certain information and assets from all types of crime. A larger number of private detectives is also needed to help lawyers dealing with criminal cases and civil litigation. The number of activities around the world grows in the context of increasing demand to control internal investigations and external financial losses, as well as to monitor competitors and prevent industrial spies (Dempsey, 2011).

A detective, in order to successfully conduct detective investigations, must constantly monitor existing regulations, constitutions, laws and other general acts regulating this matter. In order to explain the ways of performing detective activity, it is necessary to make a distinction which is the responsibility of the detective and what can and what can not be done.

Primarily, detectives deal with the collection and analysis of publicly available information, they conduct interviews with persons from the useful environment that is the subject of the research; they also with the search of professional literature; participate in various gatherings and symposiums, where good sources can be found at any time. In the Law, the detective activity involves the collection of data and information, their cooperation, as well as mediation with them in the manner established by the Law. In order to provide evidence relating to offenses or to perpetrators of criminal offenses, detectives should use rules and methods of criminal tactics. They (detectives) can collect data and conduct investigations about persons who are missing or hidden, about anonymous letters or about material damage. This means that they conduct some sort of activity of search, in all forms and tactical ways of discovering the identity of a particular person and his / her residence (search for persons), as well as for stolen or lost items (search for objects) - in auctions, the Internet, the markets, the state bodies, etc.

THE EXPERIENCE OF DETECTIVE ACTIVITY IN THE REPUBLIC OF MACEDONIA

In the Republic of Macedonia, detective activity is allowed and regulated by law. This is a relatively new activity in the country and there is a relatively small number of specialized agencies that have been approved by the Ministry of Internal Affairs for performing this kind of activity. Until recently, there were no persons with adequate education to deal with this activity (Golden Book, 2015). This was mostly dealt with by retired or former members of the security structures of the state. Detective services are often used by parents in an attempt to tackle the problems they have with their children, creditors who want to find their debtors, people who have lost some valuable item or if their motor vehicle has been stolen. In a large number of cases, the “detective” is engaged to determine the reasons for the outbreak of fire in an insured area, and it is not uncommon for companies to seek detective services to find out what their competitors are doing or to act as business spies. According to previous experience, detectives are most attractive for business people for the so-called business spyware. Numerous companies, domestic and foreign, pay very well to spy on their competition, or to track their employees who they suspect give official secrets to other companies.

As problems for the rapid development of this activity in the Republic of Macedonia, it is necessary to mention the tradition, the education of citizens in the jurisdiction of private detectives, their role in court proceedings, the organization and efficiency of the judiciary, the police and other security services, the economic power of the state and the standard of citizens, and other.

One of the problems confronting private detectives is that the appliances they use during their work are very expensive, and thus their services become very expensive. Apart from the inability to find a financial interest, the problem is that even when an unbelief or business-spyware is established, for example, the evidence obtained during the work of private detectives can not be used for court proceedings. The next problem consists in the fact that security sector reform has not yet been completed, and there are still problems in communication and information exchange between the state and private security sector. Namely, the paradigm still dominated by the state as the only legitimate actor for the use of coercive means is still prevalent. Therefore, public-private partnership encounters obstacles in the realization of mutual cooperation.

On the other hand, practice confirms that private detectives are very often more efficient than state structures, because they do not use bureaucratic manners, and pay in cash for a good and useful information they receive. The new Criminal Procedure Code, in the part of the investigation for the needs of the defense, or the new concept of a party or prosecution investigation opens an additional opportunity for the development of detective activity. In this regard, it is anticipated that the defense counsel may take certain actions during the whole procedure in order to find and collect evidence for the needs of the defense. In order to collect the necessary information, the defense attorney or the authorized private investigator (detective) can speak to persons who will present the circumstances useful for the goals of investigative actions. The defense counsel will be able to directly present information and evidence to the public prosecutor or to the judge in the previous proceedings for the benefit of the person they represent. This opens up new opportunities for the development of detective activity in the Republic of Macedonia.

COOPERATION BETWEEN A PRIVATE DETECTIVE AND THE POLICE

The cooperation between private detectives and the police, in normative terms, can be found only in Article 13 of the Law on Detective Activity, which requires a private detective to report every criminal offense prosecuted by law. The previously stated legal provision is the only thread that connects private detectives and the police. Today we can not talk about the cooperation between private detectives and the police, not only because there is not yet an adequate legal framework that determines the need for their mutual cooperation, but also because there is not yet an adequate security culture with police officers who are still in private detectives see “snouts” that correct the work of the police. Police subculture within the police community leads to the lack of trust and sense of mutual cooperation for a number of reasons, which are primarily seen in the ignorance of detective activity and its poor development in our area. The cooperation between private detectives and the police can only be achieved if there is mutual trust and mutual respect with a unique goal of preventing, detecting and proving criminal offenses and their perpetrators. The transitional period, filled with value vacuum, activated today in a corrupt period filled with great distrust in the security institutions of the system, leaves no space for cooperation between the private security system and the police. The directions in which the police and private investigators should move is in the proactive action of both segments, that is, of the actors involved in the realization of a secure community, in order to maintain public order and peace. Cooperation should also concern preventive actions in the field of understanding and profiling future crimes, as well as creating profiles of their perpetrators, and thus preventing a large number of criminal offenses. Lack of confidence disturbs the possible cooperation of both subjects, which are presented as private and state parallel systems that do not have the same goal. Private detectives are viewed with poor perception in the sense that they are people who only work for their own interests without considering the public interest.

The results of the work of private detectives can represent a large source of data extremely useful for the needs of the police, which is another reason that absolutely justifies their mutual cooperation.

THE RELATION BETWEEN CORPORATE AND PRIVATE SECURITY

A monopoly for the use of a legitimate force has traditionally been reserved for the state and its organs, and only the state is responsible for ensuring security, internal security and defending the country against external threats. However, the emergence of a new phenomenon known as the “privatization of security functions” has caused the growing complexity of contemporary internal conflicts. In this regard, comparative practice points to the processes of privatization of security functions in various areas that have been reserved for military, security and police structures in previous periods, and whose scope varies in different countries from legal frameworks, security threats and challenges, as well as from institutional capacity of the country. In this context, corporate security and security within business entities represent a new phenomenon..

In theory, there is often no clear distinction between private and corporate security, whereby common names in the definitions of corporate security are reduced to the fact that it is a planned, organized and legally conceived independent and joint function of an organization directed towards its own protection or the protection of others, and the protection of certain persons, premises, facilities, etc. It is certain, however, that corporate security can not be identified with private security, primarily because private security is actually a wider notion than corporate security. Namely, besides the private security of persons, labor and property (facilities, premises and values), private security also includes activities related to private military companies and numerous other companies that carry out a number of security related tasks on a commercial basis (Matik, 2006). This means that subjects can not, in reality, be set up within the framework of private and / or professional agencies directed to the personal protection of others, as well as the protection of certain persons, premises, facilities, labor or activities, and their activity is not exhausted in the protection and self-sufficiency, within the scope of detective activity (Kesik, 2009).

The concept of corporate security can not be equated with the concept of private security, and even less its tasks and tasks of internal security services can be identified with the facilities that are mandatory, that is, in public companies and large technical-technological systems. According to European Union guidelines, corporate security is defined as integral security, which includes security and safety, which, on the other hand, includes information gathering, security assessment and risk assessment, IT protection, crisis management for the protection from fire, explosion and damage, protection of workers' health and safety, etc .

There is no doubt that in the Balkan countries an important part of the current functioning of corporate security within the business premises is still connected to things that are in the strongest sense related to the physical and technical security of persons, property and the business of the companies of the internal factors that organize and direct these things, external and internal stakeholders who practice security. It can be assumed that the current "epicenter" of corporate security in this region is self-contained activity in large technical-technological systems, which leads to errors in defining the concept of corporate security and determining its contents. The problem becomes even more complicated due to the fact that in some business entities that have to be protected by law (banks, posters, etc.) almost all categories of private security services are represented, that is, protective and self-sufficient activities.

RISK ASSESSMENT AND ASSESSMENT OF CORPORATE SAFETY

In contemporary literature there is no single definition of what the risk is. Certain authors believe that the risk is "a situation where there is a possibility of deviation in relation to the expected result" (Emmet and Wiley, 1996); for others, it means a "measure of the likelihood that the consequences that have arisen as a result of certain dangers are harmful to life, health, property and / or the environment". Certain considerations are directed towards the definition that this is a measure of the probability of the appearance of technical or natural phenomena that are characterized by the formation and operation of the danger, as well as social, economic, ecological and other types of losses and damage (Nikolai and Nina, 2008)

Identification of persons, objects and business resources is connected with determining the basis of threats per corporation and defining whether its vulnerability can significantly affect certain phenomena in society and the state (Georgieva, 2006). Identifying external and internal threats involves recognizing the intentions and capabilities of potential threats. Internal threats include theft, sabotage, violence, vandalism, flow of sensitive information. External threats range from extreme endangering events, such as terrorist attacks and kidnapping, to something less drastic like burglaries in buildings. External threats also include industrial spyware, product contamination, blackmail, public unrest, fire, weather, earthquakes and other types of natural disasters. Assessing the possibility of the occurrence of a particular event starts from the question of the extent to which a certain perilous event can occur at all. An assessment of the possibility requires mental concentration and is not based on mathematical modules or formulas. Precise numbers are never a measure when it comes to a factor influenced by unique human behavior. Most of these analyzes are the result of knowing the nature of criminal threats, experience and common sense reasoning.

The analysis of security threats and risks is an assessment of any real or potential threat to the corporation, which can cause a person's injury or death and / or the destruction (loss) of the company's assets and / or a decrease in profits, or financial losses, no matter how large they are (Bakreski, 2011). It refers to a gradual and systematic analysis of the work and procedures resulting from the workflow of a corporation with the aim of identifying risks or threats to the company and making proactive recommendations, solutions and procedures for their elimination and / or mitigation of consequences in the event of a threat during the operation of the corporation.

CONCLUSION

Urbanization and industrialization are regularly accompanied by the rise of organized and classical crime, as well as other asocial occurrences. In this context, in the context of endangering the safety of people, property, and company work, it is certainly our influence that there is an increased number of so-called "dangerous" or "dirty" technologies, so that we can justifiably talk about new forms of crime; nuclear, ecological and others. In the sphere of economic work, the danger of accidents is constantly present, because ionizing radiation, toxic and explosive corrections and other products of modern technology are permanently propagated by destructive phenomena that can cause a number of harmful consequences. We can conclude that corporate security affects many aspects, such as the national economy, in the domain of organized crime, information security (Avant, 2007). The impact of corporate security on national security from the point of view of the economy is that corporation is an example of a complex organization in which efforts to create economic stability of the state are viewed in the context of national corporate development policies (Clinard and Yeager, 2006). Consequently, efforts should be directed towards greater interest of the state for corporations in the area of providing better working conditions, disabling unfair competition on the market, existence of an adequate control system for monitoring and inspection in that sector, elimination of political influences and manipulation, the prevention of criminalization in the part of the takeover and the provision of security services

The impact of corporate security in relation to national security in the domain of organized crime is in fact the profit that comes from illegal trafficking (often based on monopoly), smuggling, drug and arms trafficking, economic crime, etc. An important part of these assets is circulated through legal financial systems or is included in legal financial institutions or in investment in real estate, while the other part is kept or held as cash, while the third part of this money is an integral part of financial transactions of online transfers.

With this, as with other forms, it is always the intention to conceal or mask the legal nature of the assets acquired through illegal work. Similarly, corporate security has a significant impact on national security in terms of information security. In contemporary conditions, achieving the goals of the corporation is unthinkable without the effective implementation of information security. In this context, information security implies the protection of national information resources.

Each corporation can face a large number of risks, where management is crucial to adequately identify, but also to make an appropriate assessment of the likelihood that a certain risk will arise, as well as to predict the magnitude of the damage that a corporation might incur in such a conditions.

This is certainly not possible without members of private security institutions, so it is quite certain that in the coming years we will witness more and more of their importance not only in the Republic of Macedonia, but also at the regional and global level.

REFERENCES

Avant D., (2007). The Market for Force: *The Consequences of Privatizing Security,* Cambridge University Press, New York.

Бакрески О. и Милошевиќ М., (2010). Современи безбедносни системи, Аутопринт, Т.А., Скопје.

Бакрески О ., (2011). Контрола на безбедносниот менаџмент, Филозофски факултет, Скопје.

Clinard M.; Yeager P., (2006). *Corporate Crime*, Transaction Publishers, New Brunswick NJ.

Гроздан Цветковски, (2014). „Развојот *и* перспективите на приватната детективска дејност како ноу-хау професија во посткомунистичките држави", Balkan Analytica, София.

Георгиева Л., (2006). Менаџирање на ризици, Филозофски факултет, Скопје.

John S. Dempsey.,(2011). *Introduction to Private Security,* Second Edition, Wadsworth.

Hubbard W.D., (2009). The Failure of Risk Management: *Why it is Broken and How to fix it*, John Wiley and Sons Inc, Hoboken NJ.

Оливер Бакрески, Билјана Ванковска, Душко Стојановски, Александра Деаноска – Трендафилова, Стојан Славески, Стојан Кузев, Саше Герасимоски., (2014). Коментар на законот за приватно обезбедување, Скопје: Комора на Република Македонија за приватно обезбедување.

Оливер Бакрески, Драган Триван, Сашо Митевски., (2012). Корпорациски безбедносен систем, Скопје.

Славески, С., (2009).Безбедносен систем, Европски универзитет – Република Македонија, Скопје.

William C. Cunningham and Todd H. Taylor.,(1984). *The Growth of Private Security* (Washington, DC: U.S. Government Printing Office,).

Матиќ Горан., (2006). Правни аспекти физичко-техничког обезбеђења у приватном сектору безбедности", Правни информатор бр. 9 , Београд.

Кесиќ, Зоран., (2009). Приватни сектор у контроли криминалитета, Досије студио, Нови Сад.

Цхадај Д.Николаи, Подосенова С. Нина.,(2008). Управление безопасностио труда, ЦентрЛитНефтеГаз, Москва.

Laws

Закон за обезбедување лица и имот („Службен весник на РМ", бр. 80/99).

Законот за оружје („Службен весник на РМ“ бр. 07/05).

Закон за детективска дејност („Службен весник на РМ“ бр. 80/99, 66/07 и 86/08).

Службен весник бр. 12/2012

Службен весник бр. 164/13 и Службен весник бр. 148 и 193/2015

UDC 005.334:334.72(497.11)

SOME ASPECTS OF LEGAL REGULATIONS OF CORPORATE SECURITY: AREVIEW OF THE SITUATION IN THE REPUBLIC OF SERBIA

Prof.dr Milan Danićić,
Faculty for law and business studies, Novi Sad
Prof.dr Vojin Pilipović,
Faculty for law and business studies, Novi Sad

In developed countries, corporate security has been seen for decades as a strategic function of corporations and other business entities, while a system of corporative security has become an inevitable element of national security system within companies. Countries in the present time, including the Republic of Serbia, do not have an ambition to legally organize this area or to impose organizational ways and functions of corporative security to companies. Objects with critical infrastructure, for which special standards of security protection are needed, represent an exception. Functions of corporative security are partially arranged by laws from different areas (company law, criminal law, private security, emergency situations, safety and health at work, fire protection, protection of business secret, protection of intellectual property), which is also the case in the Republic of Serbia. Some international conventions, codex and standards are related indirectly to problems of corporative security.

INTRODUCTION

Even though the terms of corporative and private security are relatively long in use in ex-Yugoslavian countries, there are still certain divergences and incomprehension of their mutual relations. Sometimes they are even considered to have the same meaning, even though their functions are different (Daničić&Pilipović, 2015). However, beside their certain relatedness, there are some important differences. Private security includes not only activities related to private and personal protection according to contraction agreements, but also activities of private investigators, private military companies, private jails, and different types of citizens'volunteer actions that are directed on preservation of public security. On the other hand, functions and inner organizational forms of corporative security are in concern of companies, for whose necessities they are being performed- from classic types of inner security and protection to various counterintelligence actions, risk management, crime prevention, protection of information technology infrastructure and intellectual properties, monitoring of business cooperation and contracts with state institutions, bringing the security level within business entitiesup to the higher level (Nešković, 2017).

According to European Union guidelines, integral security is a term that incorporates security and protection activities in corporations. To be more specific, integral security includes risk assessment and management, business intelligence, information security, fire protection, safety and health at work. Unification of these activities into a one special unit within a business entity warranties efficient and rational corporative security (Banner, 1995).

Some functions of corporative security are realized through contract arrangements with entities specialized in providing service in the area of private security (Daničić, et al 2016), but a system of corporative security within business entities stillremains responsible for a wider range of sophisticated jobs, including measures and activities directed to discover and stop harmful actions, such as the ones connected to corruption, business espionage, endangerment of work and life environment, economical crime, money laundry, mobbing, as well as activities related to information technology protection, risk management and planning of steps in emergency situations etc. (Tešić, et al 2017).

When it comes to a selection of an organizational type and scope of activities of a corporative security system within a company, a special meaning is given to: evaluation of security challenges, risks and threats to functioning and business of a corporation in certain future period of time; available human resources for executing corporative security activities (Buzov, 2017);

advantages and disadvantages of the present inner security and protection system; achieved goals in the area of safety at work and protection of business environment; estimation of corporations capability to undergo criminal and corruption; estimation of threats related to industrial espionage and other criminal acts against intellectual properties; the level of safety of information technology system within a company; performance according to national laws and international standards in this area; potential endangerment of security of a company's top manager and persons included in activities of corporative security (Petrov, 2007).

For decades, western corporations have a characteristic development of corporative security functions. Part of them are known as administrative security and are linked to politics (guidelines for making decisions, which are connecting definition of corporative strategies with its usage), plans and procedures within a company. Administrative security includes informational and informatics security, tracking of business flow according to normative frameworks, safety and health protection at work, security of properties and partnerships outside the company, control and risk management, activities during emergency situations, measures of protection of intellectual and industrial properties, as well as programmes for education and raising the level of security conscientiousness of employees. Administrative security is not only under jurisdiction of a risk manager of corporative security, but it also includes other management levels within a company (Trivan,2017).

Functions of corporative security are related to activities of inner and outer security, fire protection, safety of company's management, establishment of security during some business events, enabling secure business with a state, as well as crime prevention (Cabric, 2015).

SOME ASPECTS OF GENERAL LEGAL REGULATIONS OF CORPORATIVE SECURITY

Comparative praxis shows that corporative security activities are not regulated by special laws in any of the modern states. Regulations in this area on a national level are mainly related to company's rights and to laws that are regulating issues related to private security (Mallin, 2009). Besides, certain questions from area of corporative security are better regulated by criminal and misdemeanour legislation, regulations concerning data protection, intellectual property protection, weapon and munition, fire protection, emergency situations, environmental protections etc.

Extern surveillance over subjects of corporative security in a formal way includes controlling and monitoring by competent parliamentary bodies and institutions of executive authorities, juridical control and control role of public and civil society (Lund Petersen, 2012).

In section IV of "StrategijenacionalnebezbednostiRepublikeSrbije" (Strategies of national security in the Republic of Serbia) from 2009, among others, it is stated "that a greatresponsibility for conducting activities related to inner safety lately belongs not only to state bodies and institutions, but also to subjects from private security sector, whose activities include protection of single entities, objects and other material goods, which are not under jurisdiction of state bodies". Therefore, "it is of a great social meaning that activities of these subjects are completely normative and doctrinally regulated". In the document, a term "corporative security" is not mentioned, but after text analysis it can be concluded that mentioned security jobs in Serbia, which are not under exclusive jurisdiction of state bodies, are trusted to subjects of corporative security.

Some stipulations in the Law on economic societies from 2011, which are related to jurisdiction and responsibilities of Board of Directors, show that this Board is responsible for business strategy and business goals of a business entity, for running business of the entity and determination of inner organization, monitoring of inner activities within the entity, and establishment of administrative activities, as well as risk management activities. According to legal resolution, the Board determines inner organization of the entity. Therefore, it can be concluded that it is in its jurisdiction to define organizational structure of corporative security system of business entities in Serbia.

The actual legislation in the Republic of Serbia does not know the term"corporative security". That is also the case with the Law on private security, which is established in 2013 in order to regulate the mentioned security sector. That legal act contains directives on "self-protection activities", which can be related to some functions of corporative security. After all, it describes self-protection activities as "activities aimed for provision of security of persons, properties and business, and are done by company itself", and the term "inner security service (self-protection)" is used for the organization. Here it is actually spoken about organization of physical-technical security conducted by business subject for its own needs. Other functions of corporative security are not mentioned in this or other laws in Serbia (Daničić & Pilipović, 2015).

Stipulations of the Law on private security are also regulating issues of obligatory secured objects, which are defined as objects from strategic significance for the Republic of Serbia and its citizens, i.e. as objects from special significance, whose damage or destruction would cause serious consequences on life and health of people or on defend capabilities of the country. According to this fact, the Law prescribes that protection of obligatory secured objects is done within business activities of a legal entity that owns mentioned objects, in a way that is described in the general act on organization and systematisation. That protection can be done either by contractual agreements with subjects that are licensed for offering private security services or as organized self-protective activity.

The Law on private security ensures that legal entities and businessmen could get one or more licences for performing private security activities if they fulfil taxable listed conditions, in order to organize self-protective activities, i.e. to protect their properties, business, objects, locations and employees and to establish their inner security services. (Daničić, Jovičić, 2017).

Even though the legal time limit for licencing of legal entities, which are organizing their self-protective activities, had been prolonged two times and expired on January 1st, 2017, that process is still in the beginning in the Republic of Serbia.

Historical aspects of normative regulations of corporative security in Serbia

In the ex-SFRY from 1973 until 1990, a concept of a so called social self-protection was being in effect. That concept was organized normatively by the Law on basics of social self-protection and the Law on social self-protection systems (Nikač, 2012). The Law on basics of social self-protection from 1973 regulated rights and activities of security services in the social companies, social-political organizations and unions. According to the Law, all companies were obliged to form an inner security service, while other subjects of social self-protection were responsible for organization of security of their own objects.

Goals of social self-protection in companies were disabling of illegal alienation of public properties, preventing damage,abuse of position, economic criminal and influences of enemies' forces, suppression of non-ethical business and corruption, preventing endangerment of inner organization and work discipline, as well as organizing actions during emergency situations that are caused by natural or technological disasters. A system of inner security in companies was including all components of physical-technical protection. At that time, detailed regulations in this area were then organized specifically within each company (Javorović, Šećković, 1987).

According to the mentioned Law, social self-protection was performed by inner professional controls, self-governing work controls, and by teams for physical and technical security and fire protection. Regulations for armament of security service personnel in companies were under the jurisdiction of the Republic secretariat for inner affairs and the Republic secretariat for economics. Persons, who were performing mentioned jobs, were obliged to go through a certain training for handling weapons. Breaking legal normative in this area was also meaning a rigorous punishment for legal entities and individuals. (Labović, 2015).

Employees, who were performing physical-technical security tasks in companies, were authorized to forbid entrance or access to uninvited people, to move them away forcedly, to keep back persons that were caught in doing criminal acts, to use force and other means of coercion under specified conditions, including also fire weapons (only in cases where life of the security personnel or the objects itself was directly in danger).

The mentioned Law came out of effect in 1986, when the Law on system of social self-protection was adopted. This new law regulated authorizations and jurisdiction of physical-technical security service providers in organizations of united work (originally: organizacijaudruženograda-OUR), and their position in national security system; main responsibilities of those services; conditions for use of means of coercion; recruiting and education of corresponding personneland many other issues. Regulations of this law ordered companies to establish their own security services for physical and technical protection. These services would protect objects, employees and properties from different forms of illegal and criminal actions, enabling in the same time unhindered flow of business processes. In contrast to previous legal solutions, workers in company's security service got additional rights to determine identities of persons, while regulations regarding carrying and using fire weapons were put only under jurisdiction of the Republic secretariat for inner affairs of the SR Serbia. Finally, the Law on social self-protection system also created some normative assumptions for establishment of specialized subjects in the area of security and protection, which gradually lead to creation of private initiative in this area.

LEGAL REGULATION OF SOME FUNCTIONS OF CORPORATIVE SECURITY

Normative frameworks of protection of critical infrastructure

According to the rules in the European Union, it is recommended that the same level of security is provided for objects and facilities with critical infrastructure in the state members. This could only happen if the common frameworks of their protection exists. Interests of the EU for critical infrastructure on the EU area is a logical act, as devastation or disbalance in functioning of those facilities in one country could bring negative consequences to other state members, i.e. the EU considers that protection measures are as efficient as much as the weakest link in the chain is.

According to the EU standards, critical facilities include the ones for production of electrical energy and networks for its transmission, chemical industry, nuclear power plants, production and distribution of gas and oil, telecommunication systems, water supply systems, parts of agricultural and food industry that are related to manufacturing of the most important food, remote heating systems, systems of public health and transport, public facilities, and security and financial institutions. According to this statement and to the regulation EU COM (2006) 786 final, which was adopted by the European Commission, the EU announced the “European programme of protection of critical infrastructure”, along with the corresponding European list of objects (ECI), compiled according to suggestions from the EU state members. This EU programme defines the European critical infrastructure as any resource, service, device or infrastructure of security, economic or social importance for two or more states (Lazari, 2013).

The European Parliament adopted in 2011 the Resolution on protection of critical informational infrastructure, which demands the establishment of minimal European standards related to preparedness and reaction of authorities to different obstructions in functioning, incidents and other unwanted situations, attacks and attempts of devastation of information and communication systems within critical infrastructures, and establishment of communication channels for potential risks and incidents (Daničić & Pilipović, 2015).

The Government in the Republic of Serbia adopted a supplemented and revised Decision on determination of big technical systems that are significant for defence. Following systems were included in the mentioned list: 8 systems related to traffic and telecommunication, 3 public facilities and 4 business societies, whose activities were related to energetics, one public institution and one company involved in coal production, and 12 public companies that were related to water distribution, heating energy, forest industry and radio-diffusion (Trivan, 2017).

With this revised decision, the Government defined procedures related to election, development and modernisation of mentioned systems, procurement procedures, and the way they are adjusted for defence needs, meaning that the investor is obliged to report all these issues to the Ministry of defence and other corresponding authorities. Furthermore, according to this decision the investor is responsible to hand over all needed investment-technical documentation in these cases. Two years later, the Government agreed on the Regulation on closer criteria for determination of unquestionable protection of some objects and ways of performing these tasks. This regulation describes in details legal normative in the area of protection of critical infrastructure (Labović, 2017).

Legal aspects of protection against business espionage

In countries with developed business markets it is often a case that companies, which are business partners, regulate the confidentiality issue with a contract, protecting confidentiality of business data and information. They are so called Non-Disclosure Agreements, whose stipulations normally include fines in the case that data are published in public. These types of agreements represent an efficient way of insurance that business confidential formulas, secret knowledge and other protected information and data are transmitted to business partners, i.e. protected from disloyal competition. In addition, these contracts also ensure monitoring over business partners in the case of further revealing of protected information (Fishman &Stim, 2001).

Until 2011, when the Law on protection of business secret is adopted in the Republic of Serbia, this matter was not legally regulated, while information and data of business importance, were protected only on the level of (more successful) companies. As a consequence, in many companies there were special inner acts that would define lots of extern and insignificant information as business secrets, while in the same time business espionages and publishing of important secret business information would not be noticed. Even though this law has been in the effect for more than 6 years, its effects are still really weak and far away from the original expectations.

The Law defines business secret as any information of commercial value in the case when its content is not generally known, i.e. when it is not available to uninvited persons, who might be in opportunity to earn material profit by using or transmitting that information. In order to speak about legal term of business secret, it is important that the owner of the business secret also conducts needed measures for its protection. According to the Law, any action that is performed within business activities, which could lead to publishing of content, transmission to third parties, or usage for own needs of information that are considered as business secret, without the confirmation of the owner, or in the case when illegal measures and methods are performed, is considered as punishable act of disloyal competition.

The Law on protection of business secret enables civil-legal protection of legal entities and individuals, who can submit lawsuits, i.e. initiate a certain process in front of the court, against all persons that could harm their business secrets. (Trivan, 2017).

The Criminal Law of the Republic of Serbia in its Article 240 mentions the criminal act “Publishing of business secret”, whose forms are obtaining and giving away of a business secret. Publishing a business secret also refers to an unauthorized share, delivery or some other action that is related to transmission of confidential information from the business area, while obtaining a business secret includes collection of those information in order to deliver them to an unknown, i.e. unauthorized person.

Confidential data can be presented as a business secret in regard to the whole country, some specific part of economy or just to one business subject. The term confidentiality actually means that it is about the data, which should be kept as a secret because of its character and importance. Beside that, this data is presented as a business secret according to an authority, meaning that the publishing of the secret will or could cause a damage to a business subject.

The Law on economic societies from 2011 contains certain directions related to protection of a business secret. These directions are describing obligations of persons that are performing special activities within the business entity (members of the society with a controlling role, shareholders that possess a significant part of the main capital, procurators, management and members of monitoring committee, persons who are representatives of the society and other persons, whose special obligations are described by founding act of the society).

Characteristics of a business secret, defined by the Law, are following: data, whose revelation could have negative consequences on business entity; data that are or are not of economic significance because they are not generally known; data that are not easily accessible to third parties, who would have some benefits from their usage or transfer; data that are secured with special measures by an business entity, in order to maintain the secrecy (Daničić & Pilipović, 2015).

The Law on business entities foresees that in a case when persons with special obligations towards the business entity are acting against legally established normative, a lawsuit could be submitted against them, along with a request for a damage refund. As well, these persons could get excluded from the business entity, i.e. their employment in the company may be terminated.

Normative related to emergency situations and risk management

According to the Law on emergency situations from 2009, business entities and other legal entities in the Republic of Serbia have an obligation to plan and provide measures for establishment, preparation and education of civil protection units, which are formed by themselves. Furthermore, it is recommended that they perform activities for implementation of personal, mutual and collective protection, to perform tasks in the area of civil protection, which are related to employees and material goods. Subjects of civil protection, whose activities are related to the area of health protection, education, children and social protection, as well as for other tasks, which include protection of a greater number of persons, are obliged to ensure implementation of civil protection measures for usersof their services.

The Law on safety and health at work from 2005 introduced an obligation for employers in the Republic of Serbia to create the Act on risk assessment for all working places in business entity, which includes definition of methods and procedures of risk elimination, i.e. establishment of ways and mediums of protection of employees in a company from risks related to their working places. The Act on risk assessment analyses work conditions in all systemized work places and work environment and defines priority measures for work development and risk reduction to an acceptable level. If there are risks, from which workers cannot be fully protected, employer is obliged to inform them about all details related to the risk, even about additional benefits for performing tasks on such working places, as well with possible consequences to their health.

This Act was realized by specialized licensed experts, along with representatives from labour medicine services and persons that are performing tasks related to security and health protection within business entities. There is a legal possibility to include in this process also a certain committee, whose members are chosen by employees. It is their right to ask employer for some changes in the Act on risk assessment, if work conditions on certain working places become worse subsequently (Vemić, 2017).

International Organization for Standardization (ISO) adopted on November 13th, 2009 a new standard ISO 31000, which is related to principles and methodology of risk assessment. According to the standard, a term of risk is considered to be an insecurity in realization of planned goals, while a term of risk control is introduced to define a communication and consulting process with intern and extern partners, definition of criteria for risk assessment and analysis structure, identification and analysis of potential risks, estimation and strategically planned risk analysis, as well as observation of implementation possibilities and efficacy of all phases in the risk management process, which also includes continuous improvement of measures and activities in the process (Cubbage& Brooks, 2016).

The Standard ISO 31000 is related in the first place to companies, whose activities are connected to the greater risk in the work process. Anyhow, in practice, in some business objects implementation of the standard is being continuously postponed, or only inner acts related to risk management are used, including just some elements from the Standard ISO 31000. Special advantage of the mentioned standard lies in the fact that the same is harmonized to other ISO norms, such as ISO 9001, ISO 14001, ISO 19600, ISO 27001, ISO 20000, ISO 55000, ISO 22000, ISO/PAS 28000, which enables its easier integration in IMS Integrated Management System. The Institute for Standardization of the Republic of Serbia adopted on September 30th, 2015 the first Serbian standard, whose content corresponds to the ISO 31000.

Legal regulations of corporative criminal matter

After adoption of the Law on responsibilities of legal entities for criminal acts in 2008, in the Republic of Serbia was finally created a possibility that legal entities as well can take over responsibilities for all criminal acts except the ones that could only be done by individuals because of their special nature. Introduction of these types of laws is characteristic for many national legislations in Europe. According to regulations that were valid in Serbia at the time before the mentioned law, legal entities could only be responsible for some criminal and economical violations (Trivan, 2017).

According to the law, a legal entity has a full responsibility for criminal acts from the domain of corporative criminal, i.e. for actions that are performed by authorized persons and which are targeted to create some profit to a legal entity. In this context, a legal entity is only responsible for omission of legally prescribed monitoring and control, which gave an individual an opportunity to perform a criminal act in favour of the legal entity.

However, there is a predominant attitude that the Law on responsibility of legal entities for criminal acts exist only on paper, meaning that actual persecution of criminal offenders in the area of corporative criminal is not being realized, and that other national regulations still have a selective approach to that type of criminal, including the Law on protection of consumers, the Law on safety and work protection, and many other legal acts that have some touch points with that matter (Keković, 2009).

Normative frameworks of environmental protection and fire protection

According to the Law on environmental protection from 2004, there is a definition of environment, saying that environment is a collection of natural values and the ones originated from human influence, whose complex interactions constitute a life surroundings. Stipulates from that law foresee that business entities, in the case when their business could lead to pollution and deterioration of the air, earth and water quality, have to implement legally defined conditions regarding the environmental protection every time before building object, manufacturing facilities, their reconstruction and beginning of work. (Kostić, 2009).

According to the Law on fire protection, protection measures in business entities in the Republic of Serbia are organized and performed dependent on the assessment of the degree of endangerment, as well as on the nature of technological processes in manufacturing facilities of the business entity, on characteristics of manufactured, stored and reprocessed materials, on materials used for the building of the object and on importance of the object, legal entities i.e. economic societies are classified in three groups.

First degree of vulnerability, defined as existence of high risk for outbreak of fire, is characteristic for companies that are manufacturing, i.e. using explosive materials, flammable liquids and gases, or if the objects are used for the storage of the mentioned ones. To this group are also included companies in whose objects and facilities during technological process a dust is created, which forms explosive mixtures with the air. In the end, this category also includes facilities that are characterized by grouping or connecting of flammable elements and parts, which enable fast expansion of fire, and resources of critical infrastructure.

Other category of vulnerability is defined as existence of higher risk of outbreak of fire. It includes companies that manufacture, i.e. reprocess solid fuels, non-combustible or melted metals, facilities used for storage of different types of flammable liquids in small amounts, and public objects that are used for gatherings or staying of a greater number of people.

To the last category of vulnerability, which is characterized by a certain/ determined degree of fire risk, includes all objects of business entities in Serbia, which are not classified in first two groups, but which have a certain meaning from the aspect of the fire protection (Mlađan, 2009).

The governmental Regulation on classification of objects, activities and land into different categories regarding fire threats, which is dating from October 2010, elaborates stipulations from the Law on fire protection that are related to the process of classification of objects within abusiness entity according to the criteria for evaluation of fire threats. The classification of the mentioned objects is under jurisdiction of the Sector for emergency situations within the Ministry of inner affairs of the Republic of Serbia, and it is always finalized by a solution that is valid for all business entities and other legal entities.

Depending on which category abusiness entity or other legal entity belongs to, according to the Law a general organization of fire protection is performed, meaning that:

-business entities and other legal entities from the first category regarding fire threats are obliged to form a firefighting unit with a certain number of members, a level of equipment and education

- subjects that are belonging to the second category have to organize and perform preventive measures in the area of fire protection, including permanent on-call duty by professionals;

- business entities and other legal entities, which are in the third group, have to organize and perform preventive measures regarding the firefighting protection and to have a certain number of educated professionals.

The Law on fire protection allows business entities and other legal entities, which are performing tasks in the area of fire protection, to hire through contract some other specialized business entity or other legal entity, which has an approval from the Ministry of inner affairs for performing such tasks. That legal approach in the last couple of years is a subject of many discussions. On one hand, it is hard to believe that professionals engaged in this way would truly devote themselves to these activities and adequately protect objects from fire threats. In contrast, a huge number of subjects that are included in the mentioned categorization consider that it is more rational to make an agreement on engagement of specialized units than to organize themselves these units that are foreseen by the Law. Furthermore, they add that effects in both ways would be quite similar, i.e. weak.

Comparative experiences show that this matter regarding fire protection is not even uniquely organized on the level of the European Union, while these regulations are left to the state members, with an obligation of mutual harmonization. It is characteristic for standards in the area of fire protection that they are being harmonized while working on them. The most important mechanism of the harmonization is a cooperation between reference laboratories of European countries and organizations for standardization on national levels (Jones, 2015).

Regulation in the area of information technology security

Information technology security service represents one of the most important functions of corporative security within a company, with a condition that this segment of security is also being controlled systematically, respecting the standards from the area, as well as national legislation and intern regulations within the business entity. (Daničić & Pilipović, 2015).

Since there is no unique standard that would include all areas of security of information and data bases, business entities have to follow different international standards in the area of informatics protection, such as ISO/IEC 15408, which is related to integration of requests in the domain of information technology security, ISO/IEC 113335, which concerns the control of security of an IT process, ISO/IEC 17799, the general standard in the area of information technology security that lead to a new standardISO/IEC 27k and other standards of information technology security NIST SP 800-64, NIST SP 800-30, along with NIST SP 800-53, which are originating from the United States of America (Protić, 2013).

The regulation regarding the information technology security in the republic of Serbia is still not complete, and some parts are outdated. Organization of this area is being constantly postponed, even though in the last few years some legal acts were adopted, such as the Law on free access to information of public significance from 2004, the Law on electronic document from 2009, the Law on electronic signature and the Law on registration of business entities from 2004, whose solutions enable only partially the implementation of electronic management in Serbia.

Legal protection of intellectual property

Criminal legislation of the Republic of Serbia contains a group of criminal acts against intellectual property, which include: violation of moral rights of author and interpreter, unauthorized use of author's part or other subjects with the same right, unauthorized elimination or change of electronic information on author's and related rights, violation of invention right and unauthorized use of someone else's design.

Beside mentioned criminal acts, which are systematized in the chapter XX of the Criminal law book of the Republic of Serbia, in this legal act there is another criminal act from this area- "Unauthorized use of someone else's business name and other special marks of goods or services", which is classified as an act against business from the chapter XXII K3, but is actually related to the protection of intellectual property, as it is dealing with protection of stamp rights, rights related to geographical origin and rights related to protection of topography of intellectual circuits (Trivan, 2017).

CONCLUSION

Organizational forms of corporative security system are representing an expression of available resources of a corporation, which are set up so that they achieve goals in a rational and efficient way. On inner structure and the position of organizational units in the domain of corporative security in contrast to top-management is being influenced by many factors, but the main criteria is realization of a business strategy of a corporation.

By improving their own safety, corporations are also contributing to higher level of security of a broader region. For example, electronic systems for monitoring and protection of the company itself, could also be useful for state subjects, which are responsible for enforcing the law while performing their tasks. Measures related to fire protection that are used by business entities also represent a contribution to raising the general level of environmental safety. In addition, while performing activities in the domain of corporative security, other criminal acts could be revealed, which are related to corruption, economic and ecologic criminal, business espionage, sabotages, thefts, mobbing and others.

A legal-normative framework of corporative security is conditioned by valid legal stipulations of each state, on whose territory a company is doing business. Along with national regulations, there are other regulations that have to be respected, such as international agreements, conventions, declarations, standards and similar acts. Anyhow, corporations can regulate the inner organization with internal acts independently from the legal organization within a state (but not opposite to it), as well as some other procedures and activities in some business areas, including corporative security.

Generally on corporative security in the Republic of Serbia and other surrounding states is being influenced by a state of national economies, by a business climate in these years of economic and financial crisis and in states of unsuccessful and prolonged transition process. Namely, economic difficulties, downfall of investments and employment, recession and problematic privatisation processes, just have to influence on a state of organization, motivation, loyalty and efficiency of activities of inner subjects in companies, which are in charge of certain functions of corporative security.

Beside the Law on private security as a coverage act, the significance for normative regulation of the area of corporative security in the Republic of Serbia also belongs to the Law on environmental protection from 2004, the Law on safety and health at work from 2005, the Law on responsibilities of legal entities for criminal acts from 2008, the Law on emergency situations and the Law on fire protection from 2009, the Law on business entities, the Law on protection of business secret from 2011, as well as some stipulations within the Criminal law book of the Republic of Serbia.

In the period before the establishment of the Law on private security, a significant normative framework for companies that were performing tasks related to private and corporative security was represented by some stipulations within the Law on weapon and munition, which were regulating some questions from the area. In the first place, it is related to purchase of fire weapon, education of private security personnel about handling the same, performing security checks and getting consent by the Ministry of inner affairsfor performing the security service along with carrying a weapon.

In the Republic of Serbia theoretically there is no parliamentary monitoring over corporative security, as there are no legal normative or any stipulations within the Rules of procedure of the national assembly that are organizing this area. However, according to stipulations of the Law on private security, a part of activities in economic societies related to corporative security (especially to inner physical and technical security), are being referenced to as “self-protective activity”. There are legal orders regarding these activities, which are related to legal entities and individuals, who are providing private security services according to the made contracts.

Application of these legal orders onto subjects of corporative security is mainly related to a process of licensing, monitoring by authorized police services of the Ministry of inner affairs, which points to existence of a certain type of control in this area. Ombudsman’s authorizations in this area and the application of the same in practice are insufficient and unnoticeable.

It might seem that the area of corporative security in the Republic of Serbia and other countries is escaping from radars of state regulation and that some of the aspects are functioning on the border of a grey zone, especially when it comes to multinational corporations and their branches. However, this area is too complex and branched in order to be legally regulated in a unique way, while countries with their markets cannot have pretensions to regulate everything when the business entities and market race is in the question.

LITERATURE

Banner, K.D. (1995). *Designing Effective Organizations: Traditional & Transformational Views*, SAGE Publications, Thousand Oaks CA.

Barney, J. &Hesterly, S.W. (2005). *Strategic Management and Competitive Advantage*, Prentice Hall, London UK.

Buzov, V. (2017). Krizina korporativnata sigurnost, Nešković, S. (ur.), *Društveni fenomeni i korporativna bezbednost – Tematski zbornik radova - knjiga XXV*, Centar za strateška istraživanja nacionalne bezbednosti CESNA B, Beograd, str. 1-4.

Cabric, M. (2015). *Corporate Security Management: Challenges, Risks, and Strategies*, Elsevier Science, Amsterdam NL.

Cubbage, J.C. & Brooks, D.J. (2016). *Corporate Security in the Asia-Pacific Region: Crisis, Crime, Fraud, and Misconduct*, CRC Press, Boca Raton FL.

Daničić, M. & Jovičić, D. (2017). Challenges of surveillance of the private security sector in the Balkan countries, *Security Dialogues*, Vol. VIII, No. 1-2, Faculty of Philosophy, Skopje, pp. 647-666.

Daničić,M.&Pilipović,V.(2015). Aktuelna pitanja zaštite kritične infrastrukture,*Međunarodni naučni skup „ Vrednosti i identitet“* ,Fakultet za pravne i poslovne studije drLazar Vrkatić, Novi Sad.

Daničić, M.& Pilipović, V.(2015).*Privatna bezbednost*, Fakultet za pravne i poslovne studije drLazar Vrkatić, Novi Sad.

Daničić, M., Skakavac Z.& Dragović Sekulić, S. (2016). Implications of the Ongoing Expansion of Private Security Sector, *International Scientific Conference - Private Security in the 21st Century: Experiences and Challenges*, Stedagrafika, Skopje, pp. 109-120.

Fishman, S. &Stim, R. (2001). *Nondisclosure Agreements: Protect Your Trade Secrets and More*, Nolo, Berkeley CA.

Javorović, B. &Šećković, J. (1987).*Komentar Zakona o osnovama društvene samozaštite*, Narodne novine, Zagreb.

Jones, A.M. (2015). *Fire Protection Systems*, Jones & Bartlett Learning, Burlington MA.

Keković, Z. (2009). *Sistemi bezbednosti*, Fakultet bezbednosti, Beograd.

Kostić, M. (2009). Ekološki kriminal i njegovo suzbijanje, *Pravni* život, Vol. 58, br. 1-2, Beograd, str. 175-182.

Labović, D. (2017). Normativna regulativa privatn ebezbednosti Republike Srbije – dostignuća i perspektive, *Bezbednost*, br. 1/2017, MUP Republike Srbije, Beograd, str. 115-136.

Labović, D. (2015). *Privatna bezbednost – pravna i socijalna dimenzija*, Inovacioni centar ,Fakulteta bezbednosti, Beograd.

Lazari, A. (2013). *European Critical Infrastructure Protection*, Springer, Heidelberg DE.

Lund Petersen, K. (2012). *Corporate Risk and National Security Redefined*, Routledge, New York NY.

Mallin, A.C. (2009). *Corporate Social Responsibility: A Case Study Approach*, Edward Elgar Publishing Limited, Cheltenham UK.

Mlađan, D. (2009).*Posledice požara, havarija i eksplozija*, Kriminalističko-policijska akademija, Beograd.

Nešković, S. (2017). Korporacijski kriminal i korporativna bezbednost u postmodernom poslovnom ambijentu, Nešković, S. (ur.), *Društveni* *fenomeni i korporativna bezbednost – Tematski zbornik radova - knjiga XXV*, Centar za strateška istraživanja nacionalne bezbednosti CESNA B, Beograd, str. 49-64.

Nikač, Ž. (2012). *Koncept policije u zajednici i početna iskustva u Srbiji*, Kriminalističko-policijska akademija, Beograd.

Petrov, A. (2007).*Aktivna korporativna sigurnost*, Izdatelstvo „Svят. Nauka", Sofiя.

Protić, D. (2013). Informaciona bezbednost: standardi ili pravila", *Vojno delo*, Godina LXV, proleće/2013, Ministarstvo odbrane Republike Srbije, Beograd, str. 133-150.

Tešić, M. &Tešić B. (2017). Savremeni kocept korporativnog upravljanja i funkcije korporativne bezbednosti, Nešković, S. (ur.), *Društveni fenomeni i korporativn abezbednost– Tematski zbornik radova -knjiga XXV*, Centar za strateška istraživanja nacionalne bezbednosti CESNA B, Beograd, str. 303-320.

Trivan, D. (2017). *Osnovi korporativne bezbednosti*, Fakultet za poslovne studije i pravo, Beograd.

Vemić, M. (2017). *Optimal Management Strategies in Small and Medium Enterprises*, IGI Global, Hershey PA.

UDC 005.334:334.72

CORPORATISM AS A THEORETICAL FRAMEWORK FOR THE STUDY OF CORPORATE SECURITY

Sonja Dragović Sekulić
Faculty of Law and Business Studies dr Lazar Vrkatic

Previous centuries have been marked by industrial and technological innovations and revolutions, but the 21st century is characterized by the changes that occur in the field of human consciousness. These changes are manifested in different fields of interpersonal relationships, from culture to communication, in the form of adjustments or even the full acceptance of the foreign thing. Throughout the process of these changes and events, largely enabled by the process of globalization, the most important place is taken by the "new" doctrine of corporatism. In the very essence of this doctrine are corporations and corporate interests that seek to appropriate as much power as possible on a global scale. In this process there is a weakening of the state's power and creating of the basis for corporate security.

INTRODUCTION

By the end of the Cold War and the fall of the Berlin Wall, there is a change in many areas, as well as changes in the approach to security studies. The country-centric approach to security interpretation is now abandoned, and a broader understanding of security emerges. This new approach advocates the introduction of "civilians" into the study of security and the dissemination of the concept of human security, food safety and the like. As a relatively young teaching-scientific discipline from the security science corps, corporate security is the subject of many authors' interest, and therefore the subject of scientific controversy about a unique approach to defining its concept and content. Should we start from the very term as such, we can consider corporate security from the aspect of the corporation as a form of a company in which the ownership is separated from the management function (Radovic, 2010) or the term *corpo* (body, whole) and this already points to different interpretations of this term. Although the notion of corporate security is not particularly classified, it belongs to the economic, political and social sector. Some authors identify corporate security with private security and state that this term implies *planned, organized and law-based joint activitiy and function of organizations, private and / or professional agencies aimed at protecting themselves or protecting others, as well as protection of appropriate persons, premises, facilities, businesses or activities that are not covered by the exclusive protection of state authorities.* (Stajić, 2008) Others state that this is *a strategic function of the company, which aims at achieving security of the business success of the corporation, which means eliminating all risks and threats that may affect business activities and achievement of business success, minimizing the potentially dangerous effects, business functioning in crisis conditions as well as overcoming the crisis and re-normalizing business.* (Ivandić et all, 2011)

Unlike the above, some authors define corporate security as part of a wider social security and represent it as a complex sociological system that is interconnected and intertwined with global, national and regional security systems. (Nikolić, Sinkovski, 2013) This definition is supported by the theory of sociology of security, where the notion of security is defined as the totality of the current factors that enable favorable conditions for the development of the country, life-ability and achievement of the national goal ... (Kuznetsov, 2007) To this approach we could also add the definition given by prof. dr Slobodan Marković, who states that *corporate security is a result of the social relationship of the public private and civil sector in a society organized on a corporate principle.* In addition to this, he also emphasizes the difference in relation to the concept of corporate security that is linked to a particular (single) corporation. (Marković, 2013)

Given that the differences in approaches to the definition of this very actual term are extremely large, it is first necessary to study it well and set a clear theoretical framework so that only then a common or universal definition of corporate security can be reached, that is, in order to achieve consensus in science and practice. Therefore, this paper will show corporatism as one of the theoretical frameworks and political doctrines necessary for a clearer understanding of corporate security itself.

CONCEPTUAL DEFINITION AND DEVELOPMENT OF CORPORATISM

In the original sense, corporatism denotes a political doctrine founded in the medieval, or feudal, vision of the constitution of the political community through corporations as separate organized collective political subjects. Corporatism means the application of principles, doctrines or systems of corporate association to an administrative unit, city or state, or the delegation of legal order and sovereignty to corporate structures. Corporatism represents the theory and practice of organizing the entire society into business entities that are subordinate to the state. (Markovic, 2007)

The corporate regime means that any profession, which has been previously properly organized, receives regulatory authority in the economic, social and political fields. A true corporate regime can only be considered when a legal state of affairs is built up, that is, when the managers of the corporation[1] are officially authorized to speak on its behalf, and the corporation has the right to set rules that must be observedl by all subordinate members. It exists only when the corporation forms a kind of public-law association, which in its field is prescribed by the law and imposed on everyone. This suggests that corporatism can only be developed at the expense of the individual and at the same time the power of the state. The main feature of economic evolution is the increasing power of groups, and the most difficult problems of economic and social policy are the consequence of this group's aspirations

[1] The word "corporation" derives from the Latin corpus (body), representing "a body made of men"; It is a group of people empowered to act as an individual. A **corporation** or a company is a legal person, often having similar rights as a natural person: to possess property, be indebted, to sue or be sued. Its purpose is to unify group business interests and represent the most common form of business association. In everyday, in colloquial, speech, the corporation refers to a business entity that operates in accordance with government legal frameworks. Churches, interest groups (non-profit or voluntary organizations or associations), cities and local governments (which can also be called "public corporations") also have a historically founded, corporate identity. (http://sh.wikipedia.org/wiki/Korporacija, 28.04.2013.)

to the role of the first order. This aspiration is also recognized in the struggle of corporations to rule the market instead of regulating it, with abuses of power and consumer spending as well as the exploitation of labor. As Olivier-Marten writes, the corporate organization is an attempt to rationalize distribution and production. Ehren Matton states that "the corporation should take care to preserve the competition that drives everyone to the effort and assures the role of individual interest that is the instigator of overall economic activity. Everyone must be free to sell wherever he wants and how he wants to increase his company or his business."

If we assume that corporatism in terms of production achieves a useful reform, the question is how much is the value of such a transformation if viewed from the perspective of the consumer and given the general interest, because in a state guided by the corporate principle, the actual force goes to the producer side. Manufacturers, better organized, supplied with powerful financial resources, assisted by influences in their respective jurisdictions, often manage to impose their views on the consumers' interests, and once they exercise the power of government in the social and economic order, then they are certainly exercised by the political authorities. The supporters of integral corporatism believe, contrary to the above, that the economic factor stands above the political and that only economic problems deserve to be approached to their resolution, and that political debates are empty and sterile. They also tacitly assume that the protection of the general interest can automatically come from a simple encounter of special interests. However, it is obvious that the most important issues concerning the lives of the state themselves are in fact political and that they are not reduced to problems of clean technology or to conflicts of simple material interests. Corporatism breaks down workers 'unity by placing it on as many groups as they have in the profession and damaging the workers' sense of international reciprocity, undermining the economic and social organization exclusively for the interest of the national community.

In the past, corporations had to serve the common interest and, in the first period of their creation, the confessional environment in which they were, the power of notions of a fair leap and a fair price, widespread by medieval theology, really ensured a certain consensus between corporate activity and the demands of the common good. But insofar as the society lay down and if the interests became irresistible in it, corporations were increasingly devoting themselves to the egoistic defense of the interests of their members. (Piru, 1983)

Historical development

In the 1930s, corporatism was the hallmark of the economic side of fascism, which was based on the combination of a strong centralized non-democratic government and large corporations. (Marković, 2013) However, the corporate system is not the creation of fascism. Even before that, social Catholics proposed the establishment of corporate associations. In order to prevent the strenghtening of the unions, they wanted to create instead a community of employers and workers. The corporation affirmed itself in the middle ages, in the period when crafts were at the economic peak. These corporations were made by masters of the same crafts, and they had a monopoly of processing and sales, as well as all the governance in the corporation.

In the beginning of fascism as a movement it had the sole goal of taking power, and when it succeeded, they tried to reorganize economic and social institutions into a social life of the new form. To this end, it is emphasized as the most important element of fascist ideology, the corporative organization of the state. (Markovic, 2007)

Considering the diversity of ideological trends and political regimes in the countries that carried out the corporate organization, it can be concluded that it is not possible to determine or realize a single type of corporate organization. Corporatism seeks to create a system in every country that will be a true reflection of the real state of social forces, cultural progress, material possibilities, and social relations, and that will meet the needs that arise from this state. In addition to all the differences, however, there are certain related elements between the corporate system of the organization so that, with certain criteria of judgment, a division of corporate organizations of different countries into certain types can be made. Criteria that are taken into consideration are: forms and methods of organization, goals, subject and area of corporate organization, etc. According to the criteria of the forms and methods of organization, given the political regime, corporate systems are divided into democratic (Christian-Social, Socialist-Syndicalist) and authoritarian (fascism, national socialism, universalism).

Italy

The Italian corporate order was established only after the fascist state conquered the trade unionism, which was a necessary condition for the establishment of corporations. The corporate movement in this country has evolved according to current needs and circumstances, regardless of any pre-determined doctrine. Although fascism claims that there is no "economic man", but an "integral man" who is a synthesis of political, economic, religious, world, and warlike, it still sets the corporate system to differentiate society under the exclusive influence of the economic factor. For fascism, state is an absolute value, while individuals and groups of relative values, that is, individuals and groups, moral and cultural aspirations, initiatives and work, spiritual and material wealth are in the fascist state the public category and functions whose value is determined by the interest which they represent for the state.

The Law of 03.04.1926. did not establish either mixed trade union of the corporate order but the foundations for further building of working and economic relations in the direction of corporate governance of the state were laid off. Regulation of 01.07. of the same year specified the competencies of these corporations and gave them a certain legal form. It was the first time that the word *corporation* was used in Fascist legislation. The jurisdiction of these corporations extended to:

1. Reconciliation of disputes between subordinate unions,
2. Initiating and supporting all initiatives aimed at better organization of production,
3. The establishment of a liaison body everywhere where the need is indicated,
4. Establishment of compulsory general legal norms for professional training and supervision of their implementation.

All these new concepts of fascism about work, production, man and labor relations were codified by the Charter of Labor on April 21, 1927. The charter is formally divided into four parts: the corporate state and its regulation, collective agreements and wages, labor markets, social welfare, professional development and upbringing. The charter also delineates the private sector from the public: "The corporate state considers a private initiative in the field of production as the most efficient and useful tool of the nation. Since the private production organization is a function of national interest, the company manager is responsible to the state for production management"; however, state intervention is limited to 3 cases:" State intervention in economic production occurs only when a private initiative is absent or where it is insufficient or when it comes to the political interests of the state. The intervention may be in the nature of surveillance, assistance and direct management." With this charter, corporations were defined as joint organizations of productive forces which fully represent their interests, and if one takes into account that the interests of production are also national interests, then the corporation is recognized by the law of state authorities. Such a corporate system was completed by the law of March 30, 1930. which established the National Council of Corporations which had a triple jurisdiction: normative, advisory and hierarchical. After the founding of this council, there is a four-year gap in the further building of the fascist union-corporate system. The framework for building corporate governance was created, but it started to really function only after the law was passed on February 5, 1934. The reform of the Italian economy on a corporate basis has, among other things, enabled the state to better defend and strengthen the positions it has gained in the economy. This reform was to be achieved in the first place by disciplining the economy, and under that term, a kind of controlled economy was controlled by the state. By reorganizing the economy on a corporate basis, fascist atuhors wanted to achieve the following goals:

1. Mitigation of competition, which would strengthen the position of the enterprises in which the state is represented,
2. Easier implementation of measures of general benefit, which in many ways facilitated efforts for autarky,
3. Comparison of opposing interests in order for the regime to more easily find a common interest and
4. Reducing social disparities by promoting the interests of the workers themselves for business issues.

Through the Law of 19.01.1939. by which the Fascist and Corporate Assembly was established, corporations were introduced into the legislative body by which political and economic legislative powers were merged. Although Italian corporatism is formally based on a tripartite legal relationship (employer, employee, and state), in reality it is a bi-partite relationship of subordination between the state and the employers on the one hand and workers on the other. In the period of fascism, Italy was corporate only because it had corporations, but the society rested on the solidarity of economic functions whose needs and will was still interpreted by the state. It follows that Italian corporatism is a means of governance, but as such it is in the service of politics and state thought, and therefore it is subordinate to it. (Pejčinović, 1940)

Portugal

When a new regime was introduced in Portugal, prerequisites for regular economic growth and development that were left to the initiative of the private owner were created, but provided they were organized so that together they could lead the economy together and regulate social relations in their favor and benefit the entire nation and the state. It has already begun to hint at the new principle of social, economic and political reform of the state - a corporate principle. Salazar[2] presented the ideology of the new social organization in his speeches and in the legal form it was presented in the Constitution of 19.03.1933. and the Statute of National Labor. The ideas of leading the new social order were the following: the idea of nationalism and patriotism, the idea of social solidarity and corporatism, and the idea of spiritualism.

A corporative organization on a social basis contains the participation of all the structural elements of the people (family, profession, municipality) in administration and drafting of laws - an organic corporate principle. This principle is the most important in the construction of a state under the new constitution. According to him, in the life of a state the decisive role belongs to social units. The new constitution also regulates the organization of power in legislative, administrative and judicial matters. Legislative power is exercised by the National Assembly, but no legal proposal can be placed on the agenda if it has not previously passed through the Corporate Chamber. Salazar emphasizes that he wants to create a corporate state, and the Constitution explicitly states that Portugal is a corporate state. Regarding the activities of the corporations themselves, the Constitution and the laws state the principle of as much freedom of censorship and their self-governance as the principle of subsidiarity, giving the state authorities only the completion of their ac-

[2] Antonio de Oliveira Salazar, was a Portuguese professor and politician who served as Prime Minister of Portugal from 1932 to 1968. He also served as Acting President of the Republic in 1951. He founded and led Estado Novo (New State), an authoritarian, right-wing government that chaired and controlled Portugal from 1932 to 1974. Contrary to communism, socialism, anarchism and liberalism, his rule was corporate, conservative and nationalistic.

tivities by co-ordinating, encouraging and managing social activities for the purpose of realizing a fair fund of interests within the limits of the legal subordination of individual interest in general. However, while emphasizing the principle of economic freedom, the state has an important role in economic relations. On the one hand, it guarantees the widest scope of private property rights, and on the other hand it seeks, in the public interest, that the national economy generates the maximum of production and wealth that are socially beneficial, and to organize a common life. (Šćetinec, 1938)

Switzerland

In Switzerland there was a developed corporate organization from the second half of the Middle Ages to the beginning of the 19th century. After a century of liberal regime, the interest in the renewal of a professional corporate organization began to awaken. In 1918, the first corporation was established voluntarily, and then other corporations of different professions started to form. By 1935, 20 corporations were formed that were composed of trade unions and employers' unions and which were affiliated in two federations. Since they were voluntarily founded by the trade unions, these private law organizations are completely independent from the state.

Holland

In Holland there was a strong interest in the corporate organization after the World War I. This interest was initiated by a quasi-corporative organization of the graphic arts craft that has encouraged Christian unions to try to implement the corporate organization and other economic categories voluntarily. In 1919, trade unions of workers and employers established common bodies for the area of industry, trade and agriculture that had the significance of a voluntary corporation.

Belgium

Belgium is one of the countries with a strong corporate tradition because corporations were active from the 11th to 17th centuries when they were dissolved by the French authorities. Regardless of the formal dissolution of the corporation, there remained strong corporate spirit.

France

France is the classic country of liberalism that, since 1789, has first dissolved a corporate organization and banned any professional association. However, the idea of the renewal of the corporate organization appeared very early, and it was especially present after the end of the war. Different movements and currents build the foundations of a corporate organization on a democratic basis.

Corporative doctrines

In terms of the classification of corporate doctrines, there are different opinions in theory, but one can note the five consistent concepts of corporate theory:

- *Catholic social doctrine* - advocates of corporatism from the end of the 18th and the beginning of the 19th century mostly discussed the issues of forming representative bodies, and completely ignored the role of the state. The ideas of corporatism that developed within the framework of this doctrine had two important characteristics. The first is the fluctuation to declare bodies formed on the basis of belonging to a particular profession in one form of representation. The other is that these theoreticians equaled corporatism with the medieval system of the class assemblies as an effective means of mitigating class conflicts and improving the living conditions of the poor.

- *organicist theories of the nineteenth century* - the ideas of corporatism contained in these theories are in the effort to ensure that industrial organizations control society because the industry is making progress, the means of mass survival and an eye for abundance, and thus it is the key point based on the unity of the class of industrialists and the class of industrial workers. This unity implicitly leads to the idea of unionism, and that which influences the decision-making process of the government. This type of labor syndicalism has largely influenced the later concepts of corporatism that attempted to organize a national economy based on corporations that will be controlled by the state, in which capital and labor are represented. A prominent theorist of corporatism within the framework of this theory was Emil Dirk, who considered that corporatism provided enough discipline to regulate the wishes and requirements of those who do not restrict themselves. Gathering its members into an integrative whole, corporatism forces the individual to act in accordance not only with his goals, to make concessions and compromises, and to take more interests into account than his own.

- *revolutionary syndicalism and gild socialism* - these theories arise with the emergence of workers' unions under the strong influence of anarchism. Revolutionary syndicalism was primarily aimed at the demolition of the state and its replacement by the union of trade union organizations that would be formed for every industry while gilded socialism emerged as its outlet, but advocated a society that would constitute federations of self-governing workers' organizations for certain trade unions. Gild socialism was focused on decentralization and the provision of autonomy to functional bodies.

- *authoritarian corporatism* - the beginning of the twentieth century marked the breakthrough of individual corporate ideas in the way that organizations of certain political institutions were organized, but these ideas could not be realized primarily because of the economic and social conditions that had not yet matured for their realization. The common thing in the first half of the twentieth century both for the corporate theories and attempts to apply them was radical authoritarianization of the concept.

- *corporatism as a substitute for parliamentarism* - one of the basic views of all corporate doctrines is that it is better for legislative bodies to be composed of delegates from organizations formed on a professional basis than representatives of political parties elected on the basis of a territorial principle. The common premise of all these theories is that the harmonious relationship of classes and organic unity is the most important for society. The social foundations of this doctrine was found in the idea that a national state represents the highest form of collectivity of a community. (Obradovic, 1992)

CORPORATISM AND NEW WORLD ORDER

Throughout the centuries, the debate about corporatism was related, directly or indirectly, to the medieval system of esnafs. As a collective body (lat. Corpora), the medieval guild served in multiple ways as economic, social, cultural, religious and political functions and for their professional membership. Among them we find the setting of standards of quality, prices and salaries, educational and working standards, care for widows and orphans, representation in city services, court services and city police, maintenance of charitable institutions such as hospitals, orphanages, poor homes and much more . With the rise of the modern state and the capitalist economy, these tasks become the subject of royal law, state administration, or market.

Together with the anti-market thinking of medieval culture, there was also the view that the state's rulers had a key role in promoting social justice. Thus corporatism is formulated as a system that emphasizes the positive role of the state in guaranteeing social justice and suppressing the moral and social chaos of stance that follows its own interests. Private companies are tolerated within certain limits, and large state projects are justified. Corporatism was once termed the Third Way and the Mixed Economy, the synthesis of capitalism and socialism, but it is actually a specific political-economic system.

The collapse of medieval corporatism emerged at the turn of the 14th century. Periodic plague, severe hunger, and extreme weather, as well as the spread of Renaissance humanism and reformist ideas of religion, science and society, began to shake off the old corporate order of the Middle Ages and open the way for an increasing emphasis on individualism, a centralized territorial role and a secular supremacy.

In addition to being a theoretical concept and type of regime, corporatism is perceived primarily as a political ideology just like liberalism and socialism. Among contemporary secular ideologies, it is not only the oldest but also the most diverse and most consistent ideology. It is difficult to draw a clear line of the separation of corporatism against individualist liberalism and collectivist socialism, as corporative thoughts and methods have taken over the elements of market liberalism as well as economic planning. (Czada, 2011)

Deeply rooted in the theory of interest organization, which in the 1960s was sovereign in political theory, the concept of corporatism in liberal democracies emerged as a basic study of Western European systems, and even of American society. The theory of corporatism that emerged in the first half of the seventies has made a strong, perhaps the strongest impact on political studies in general at this time, and its impact has remained remarkably strong to this day.

The start of a corporate concept as the theoretical methodological framework for the study of the most developed capitalist countries, emerged within the framework of the theory of interest groups that developed under the umbrella of functionalism. The use of this term within them was related to the part of these theories concerning the conditions and consequences of the creation of various forms of relations between government and society, where the interest groups played a significant role. It was most often applied to the manner of organizing stakeholders in general and the form of their involvement in the process of making government decisions. (Obradovic, 1992)

As previously mentioned, corporatism, in its original meaning, signifies a political doctrine that is grounded in the medieval vision of the constitution of the political community through corporations. The basic doctrines of the doctrine are: corporate political subjectivity, corporate presentation and threat to state sovereignty. The starting point for a corporate (re) presentation lies in the fact that the state as a political community is not established by the presentation of individual wills, but by linking corporate organized group interests. Interest groups often appear in practice as a reaction to the ideas and practice of the omnipotence of the state and the political structure that governs the state. From the end of the 20th century, corporatism is an extremely important stage in the development of a society with a great influence on its future physiognomy. It initiated major processes in the transformation of society, from reforms in the public and private sector to proprietary and political reforms with projects of standardization of the industry and services sectors, economic integration and harmonization of legal systems. All these processes are accompanied by phenomena of criminalized behavior in all social structures.

Approaches to corporatism

The contemporary theory of corporatism, long ago conceived within the framework of the theory of interest organization, retained elements of its functionalist origin in today's developed form. Their focus on the organizational structural elements of the political decision-making process, insisting on the group as a basic social unit, are undoubtedly related to their emergence within the interest groups, so it is understandable that modern theories of corporatism retain functionality as a general and theoretical approach It is inherent to theories of interest groups.

Although they have a certain consistency, contemporary theories about corporatism have nevertheless developed several directions for the definition of this term, but those are more or less differences between the author's perceptions. Thus, according to Alan Cawson, it is possible to notice the three basic directions within which corporatism is defined as:

1) A new system of political economy different from capitalism and socialism,

2) The form of a state within a capitalist society

3) The form of regulating the state-society relations, ie the form of the political system, where emphasis is placed on organizing interests and their interaction with the state..

In a somewhat different form, this division can be found in Pempel and Tsunekaw's work. Apart from approaching corporatism as a form of political system and the form of an economic system, they consider that there is also a third approach that perceives corporatism as a certain way and the relation of production. Heisler also cites the three dominant models of corporatism:

1) Using the theoretical framework (especially the theory of organization) to reflect the problems of organizing interests in politics

2) State corporate and subsidiary social corporate model and

3) An inductive approach that focuses on the mutual relations of interest organizations and government.

Much broader classification of contemporary interpretations of corporatism is given by Michael Poole, who defines corporatism in eight ways, namely:

1) a special economic system,

2) the structure of the participation of stakeholders in the decision-making process,

3) a system of negotiations between government agencies, employers and trade unions

4) type of interest representation based on state and social premises,

5) the form of the state,

6) a part of the state in a certain mode of production,

7) relationship between interest organizations and authorities and

8) the relationship between organizations and political institutions.

Despite the large number of variations and diversity in defining and dividing, all theories about corporatism can be gathered around several common points, which are:

1) the understanding of corporatism as a phase in the development of capitalism, caused by structural changes in the mode of production, where

the integration of the working class into the system represents its essential character,

2) pointing to the existence of different types and levels of corporatism, with the most divisive segments of state and social corporatism as well as macro and meso corporatism,

3) insisting on tripartism of the state, capital and labor and their cooperation as a key relation of corporatism,

4) highlighting the income policy as the main indicator of corporatism,

5) pointing to the state of well-being as an effective means of incorporating the working class into the system, controlling it and reducing capitalist labor costs for labor,

6) the explanation of the notion of corporatism is always made in relation to pluralism and

7) the perception of corporatism as a tendency in the political system and the point of its instability and cyclicality.

However, if we ask the question of security as a situation in such a society, we would say that security represents a harmonized state of political and economic interests in the model of social development conceived in such a way.

Corporatism as a form of economic system

Such an understanding of corporatism is primarily associated with one of the pioneers of modern corporation theory, Winkler. According to him, corporatism is an economic system in which the state intensively directs pre-dominately private business towards four goals: order, unity, nationalism and success. Its essence as an economic system is private ownership and state control. (Winkler, 1976) According to its advocates, the emergence of corporatism requires a qualitative change in the role of the state in relation to structural changes in politics and administration. The corporate decision-making process has primacy, while the political dimension of relations between the state and society is ignored. (Marković, 2013)

Corporatism as a form of state

The basic point of view of these theories is that corporatism is the kind of state in which the functions of representation and intervention are integrated in state institutions. That is, corporatism is such a form of state in which representation and intervention are merged into one institution - a corporation - which is constituted on the basis of the economic functions of its members. Thus, the corporation represents the interests of its members at the same time and acts as a means of implementing government policy. Unlike Winkler's view that, in corporatism, states control private capital, Jessop believes that social formations have the power, not the state, making no distinction between the power of the state and the power of the class. He further states that corporatism has the ability to keep class conflict within the state apparatus in order to prevent social reforms and ensure continued hegemony of capital. (Marković, 2013)

Corporatism as a political system

The perception of corporatism as a form of the political system, or as a form of interest mediation, is represented by the largest number of representatives of modern theories of corporatism. According to this theory, corporatism is defined as "a system of representation in which constituent units are organized into a limited number of special, compulsory, non-competitive and hierarchically organized and functionally different categories, recognized or selected by the state which guarantees them a monopoly of representing the appropriate categories in the negotiations in exchange for retaining some control in the choice of their leaders and in articulating requests and giving support." In addition to this definition, there are others who point out that corporatism is more than a special form of articulation of interest, but that it is an institutionalized form of policy-making, in which large interest organizations are one with the other and with the state authorities, not only in articulation or even in mediating interests, but also in the authoritarian allocation of values and in applying this policy. (Obradovic, 1992)

Neocorporatism

Neocorporatism, as a political doctrine, emerged in the 1970s and relates to pluralistic modifications of liberal-democratic political theory but complements them with some of the elements it assumes from the corporatist tradition - it pays special attention to the political functions of the self-organization of social and / or professional group interests and completely rejects the idea of an exclusive state sovereignty in favor of constructing a political system as a network of complementary, functionally specialized public and corporate-social organizations. Concepts of corporatism and neo-corporatism are also used as analytical terms in critical political science to reflect the contemporary transformation of a liberal civil society. (Markovic, 2007)

Unlike state corporatism, which is constituted in the case of the intervention of subordinate states, where the line between private and public is diluted, based on the hypothetical harmony of the various interests that coexist in it, neo-corporativism is created from the social dynamics, it creates and preserves autonomy of collective actors. In a neo-corporative phenomenon, structures, even in their specific, exclusive and monopolistic dimensions (which are also part of its conception), derive from a contract between substantially voluntary associations of interests that seek to reach a consensus in order to limit the inter-associative conflict or the competitive dominance of some them. The neo-corporate model covers only a part of political and economic social relations, and is linked to a system of parliamentary representation that is in line with the principles of liberal pluralism. (Marković, 2013)

Still, neocorporatism can not exist without some tacit consent or participation of the state, which gives recognition, encouragement, support and promotion to private actors, but does not answer to them, does not colonize them and does not allow others to do so.

The basic thing that allows such a model, in addition to democratic and liberal beliefs, is that the state is strong enough to preserve its autonomy from private interests, but not so strong (when applying its understanding of how to connect with those interests) to operate without the participation of the organizations that represent them. Each side has enough strength to prevent someone else from realizing one's interests one-sided and each is sufficiently weak that, if necessary, indirectly, mediate the state in order to fulfill its interests. What distinguishes neo-corporatism from old state corporatism is that it is not influenced by the political design of the state, but by a multitude of simultaneous causes arising from the evolution of civil society, from the capitalist economic system and the state itself, as well as the social dynamics that creates and preserves the autonomy of collective actors. (Goldin, 2013)

Neocorporatism is also described as a cooperative relationship between the authorities and individual interest groups. In this model, cooperation serves to maintain stability in procedures in the development and implementation of policies. Neocorporatism focuses primarily on economic policy. Three sectors of society, business, work, and government are involved in policy negotiations, and an institutionalized negotiation process between representatives of these key sectors is called mediation. The basic element of corporatism is that the government gives away the monopoly in advocacy at the top of the association in exchange for their cooperation in policy development. (Thomas, 1993)

Mechanisms of corporation governance

"Those who run global corporations, for the first time in history, seek to govern the world as a unique economic entity by means of appropriate organization, technology, money and ideology." (Richard Barnett and Ronald Müller, Dometi globalizacije, 1974) (Klark, 2003)

About 47 of the 100 strongest economy systems are represented by multinational corporations, of which only 1% owns half the total amount of foreign direct investment. At the same time, due to free market and free trade, conditions have been created for multinational corporations and banks to freely transfer capital, technology, goods and services worldwide without being covered by the laws of individual national states. This suggests that there has been a major shift in the center of power from the hands of national states to the hands of multinational corporations and banks, and today, it is precisely those that govern the lives of most people on earth. In most industrial countries, business committees, made by the chief executives of the largest corporations and banks, have created new associations between corporations and states. When leading multinational corporations agree on concrete measures, strong lobbying begins and campaigns related to key issues of established policies are launched.

Creating a globalized consumer culture is another key factor in corporatism, as multinational corporations tend to sell their products essentially with the same commercial anywhere in the world. In addition, there are also globalization of financial markets, global industrial production, global distribution of products, resource control, etc. (Klark, 2003)

Acceptance of corporatism requires us to interrupt and shake the legitimacy of an individual as a citizen in a democratic society. The outcome of such denial is the increasing imbalance that leads to the worship of personal interest and the denial of the common good. The total effects of corporatism on an individual are passivity and conformism in those areas that are important and nonformality in those that are not. One of the related characteristics of this unconsciousness is the growth of illusion. The corporate movement was born in the 19th century as an alternative to democracy and advocated the legitimacy of the group above the legitimacy of an individual citizen. The moment of glory was experienced under Mussolini and other dictators, and the last thing that today's neo-corporatists want is to to be associated with these dictators. Most intellectuals who today impose this social formula are recognized university professors - political scientists, sociologists and economists all over the West. In addition to various great ideological passions, the people suffer from what can be called fashion - from nationalization, privatization, debt financing, inflation suppression, and the like. Fashion is nothing but the lowest form of ideology, and each of these small ideologies disturbs and destroys lives but also gives the opportunity to individuals to earn wealth. The globalization and the borders that it imposes represent the most modern miniatures of the ideology of our time.

Today's society is generally based on the relationship between groups, some of them are real businesses, some are business groups, some are professions, some are state and some are private. The point of such an arrangement is that society is seen as the sum of all groups and that the primary loyalty of an individual is not a loyalty to a society but to his or her group. Serious, important decisions are not made through democratic discussion or participation, but through negotiations between relevant groups based on expertise, interest and ability to impose a will.

Another mechanism of corporatism is language. Our language is generally divided into two parts. There is a public language - huge, rich, diverse and more or less impotent. There is then a corporative language, connected with power and action, and it is divided into three types: rhetoric, propaganda and dialect. Dialects of social sciences, medical dialects, scientific dialects, dialects of linguists, artists, thousands that are inaccessible to unskilled persons and represent walls that protect the sense of importance of each corporation. Rhetoric describes the public face of ideology and propaganda is selling, "The mass does not have to know, it must believe" (Musolini). One of the characteristics of propaganda is that wherever possible music and images replace words, while for rhetoric language is essential because it is used to establish false parameters.

Corporatism surely creates a conformist society and in fact it represents a contemporary form of feudalism. The corporatist idea that elected representatives should only represent the interests led to the pressure applied directly to politicians, which resulted in the growth of the lobby industry and the turning of elected representatives to the special interests of the lobbyists. Once this principle of "legalized" corruption is accepted, it turns out that its methods are inexhaustible. In this way, the corporatist system breaks its way directly through corruption and indirectly through the damage caused by the citizen's respect for the representative system.

The mechanism that certainly comes handy to corporatism is technology. Without technology, capitalism, free markets, money markets, free trade and globalization, the people would certainly not be able to finance and maintain the existing standard of living. However, the question arises whether the very industrial revolution is the one that has raised the standard of living and has made progress unprecedented in history. It is sure, however, that it has brought progress to the new class of owners and managers, while all the others, despite all the harder and longer work, were getting poorer. The long-term pattern of the industrial revolution was to establish a lower financial standard of living and a deterioration in living conditions. The result of this was the entire century of unhindered social deterioration and disorder.

An extraordinary thing related to corporatism is its inherent power. Today, the world witnesses the third, or even fourth race for the power in less than a century. Although it is repulsed every time, corporatism every time, a few years later, reappears, transforms and grows ever stronger. (Ralston Sol, 2010)

CONCLUSION

Created at the time of the existence of guilds, corporateism re-actualized itself with the emergence of fascism and returned to the contemporary political and economic scene at the end of the 20th century. Depending on the areas in which it appeared, it had different forms and characteristics, but today it appears at a global level and involves representing the interests of a small number of elite and, of course, corporations owned by the same elite. Corporatism represents a concept of society more static than dynamic, more conservative than advanced, it is a means of subordinating consumers to the producer, employee to the employer, social to national.

Contemporary corporatism as well as corporate security is characterized by the relationship between interest groups and the representation of their interests. Once those were the interests of employers and trade unions, today they are interests of multinational and transnational corporations as bearers of economic power. The way of realizing these interests is reflected in the process of globalization. Economic, political and cultural globalization have affected the biggest and most important aspects of the lives of both men and the state. Economic globalization brings man in every respect into a dependable and subordinate position to the corporation - when going to work, when buying food, drugs, when watching television. Through political globalization, corporations realize their interests at the state level, through lobbying politicians. In this way, laws are adopted that support the most powerful and tailor the fate of every nation on the planet. Cultural globalization enables equalization of the taste and opinion of the entire world population so that one product can be sold anywhere in the world with a single commercial.

REFERENCES

Czada, R. (2011) Korporativizam(korporativizam), *International Encyclopedia of Political Science,* London

Goldin, A. (2014) *Corporatism, Neo-corporatism and freedom of association*, preuzeto sa: https://corpus.ulaval.ca/jspui/bitstream/20.500.11794/13532/1/autonomie_collective_et_droit_du_travail.pdf#page=123

Ivandić Vidović D, Karlović, L., Ostojić, A. (2011) *Korporativna sigurnost*, Udruga hrvatskih menadžera sigurnosti – UHMS, Zagreb

Klark, T. (2003) Mehanizmi vladavne korporacija, *Globalizacija*, (priredili: Džeri Mander i Edvard Goldsmit), Klio, Beograd, str.289-305

Marković, S. (2007) *Korporativna i industrijska bezbednost*, USEE, Novi Sad

Marković, S. (2013) *Korporativna i korporacijska bezbednost*, USEE, Novi Sad

Nikolić, M., Sinkovski, S. (2013) *Korporativna bezbednost – osnove zaštite biznisa I preduzetništva*, Banjac grafika, Beograd

Obradović, D. (1992) *Korporativni politicki sistemi: korporativni pristup*, Institut za međunarodnu politiku i privredu, Beograd

Pahll, R. E., Winkler, J. T. (1976) *The coming corporatism*, New society

Pejčinović, P. (1940) *Italijanski korporativizam*, Sloga, Beograd

Piru, G. (1983) *Korporatizam*, Soko, Beograd

Radović, M. (2010) Korporativno upravljanje, Fakultet za pravne i poslovne studije, Novi Sad

Ralston Sol, Dž. (2010) *Nesvesna civilizacija*, Karpos, Beograd

Šćetinec, J. (1983) *Korporativizam i demokracija*, autor, Zagreb

Stajić, Lj. (2008) Pravni okvir private bezbednosti, *Zbornik radova Pravnog fakulteta u Novom Sadu*, 1-2/2008, Pravni fakultet, Novi Sad, str. 383

Thomas,S.(1993), *First World Interest Groups, A Comparative Perspective*,Westport: Greenwood Press, http://xroads.virginia.edu/~ma98/pollklas/thesis/works.html#thomas

Trivan, D. (2012) *Korporativna bezbednost*, Dosije studio, Beograd

Кузнецов, В.Н. (2007) Социология безопасности, учебное пособие, МДУ им. Ломоносов

UDC 378.6:355

FOCUS OF PRIVATE HIGH EDUCATION FOR SECURITY ON CORPORATIVE SECURITY

Prof.dr Božidar Forca
Faculty of Business Studies and Law of the
University „UNION - Nikola Tesla" in Belgrade

From a number of aspects of security understanding, this paper focuses on national security, especially on one of its most important contents - higher education. Higher education for security in the Republic of Serbia is an integral part of higher education in general, and is realized at higher education institutions. In this paper emphasis is placed on private higher education, ie its basic contents and programs. By applying a comparative method, content analysis and case studies, the research found that corporate security is present only in fragments as a study program at private higher education institutions. Numerous reasons indicate the need for private higher education institutions in the field of security education to concentrate mainly on corporate security.

INTRODUCTION

The security of one state, or state (national) security, in theory, is most often viewed as a state, organization, function and system [Stajić, 2013; Mijalković, 2011]. Such an approach to national security is justified from the general and national aspect, in terms of prevention and repression, or the creation of a mimimum of the security of the country in the protection of its vital values and interests, in the conditions of the operation of numerous internal and external sources and holders of security threats. Understood in that sense, the state's security requires the existence and functioning of an adequate security system, with clearly defined functions and organization, which is regulated normatively. In accordance with the above, the national security system of the Republic of Serbia is defined as follows: The national security system represents a normative, structurally and functionally regulated whole of the elements of the activity from which it protects the national interests of the Republic of Serbia [*National Security Strategy of the Republic of Serbia, 2009*].

Every system, including the security system established in a country, has its own conceptual bases, which are often regarded as theoretical, political, constitutional and legal and international [Forca, 2017]. These basics directly determine the starting points in establishing the security system, its functions, organization (structure) and functioning in practice. For all the above-mentioned conceptual bases of the national security system, knowledge and skills of the human factor are needed, as the main subject of the system.

Knowledge and skills of a human factor are acquired by education. In principle, education can be observed two ways - education and training. On the other hand, education can be seen as an institutional and non-institutional activity. Institutional education activities are carried out in institutions, from the lowest to higher education institutions. Non-institutional or lifelong (permanent) education is realized by each individual, using different methods and techniques. On the third side, education can be accessed from the aspect of wider (general) education and more specialized education for a particular profession.

Higher education in the Republic of Serbia, especially for security, is in the focus of this paper. Higher education in the Republic of Serbia is carried out in higher education institutions, which, according to the latest *Law on Higher Education*, can be: university, faculty, academy of vocational studies, college and college of vocational studies [*Law on Higher Education, 2017, Article 43*]. Also, according to the *Law on Higher Education*, an independent higher education institution can be established by the Republic, legal and natural persons [*Law on Higher Education, 2017, Article 51*].

In the Republic of Serbia there are several universities and other higher education institutions, founded by the Republic, legal entities and individuals. When it comes to security, it is a fact that more and more higher education institutions opt for this activity and profession. Therefore, the primary aim of the research for the purposes of this paper was to look at the security study programs at individual higher education institutions. In doing so, the research is focused on higher education institutions in Belgrade.

HIGHER EDUCATION INSTITUTIONS FOR SECURITY IN SERBIA

The ratio of state and private universities and higher schools in Serbia is presented in Table 1.

Table 1. *State and private universities and colleges in Serbia*

STATE	PRIVATE
• University of Belgrade • University of Arts in Belgrade • University in Novi Sad • University in Nis • University of Kragujevac • University of Novi Pazar • University of Defense • University of Prishtina with current headquarters in Kosovska Mitrovica • High School for Vocational Studies • Criminal Police Academy	• Alfa University • European University • International University of Novi Pazar • Pan-European University Apeiron • Educons University • Metropolitan University • University Privredna akademija • University Singidunum • University Union • University "UNION - Nikola Tesla" • John Nesbitt University

Source: http://www.edufair.rs/fakulteti/

According to the data in Table 1, there are more private than state universities and higher schools in Serbia. If we look at the situation in Belgrade, then the situation is as follows: 1) out of 10 state universities and higher schools, five are in Belgrade, 2) out of 11 private universities, eight are in Belgrade, and the remaining three are in Novi Pazar, Novi Sad and Sremska Kamenica. Therefore, the vast majority of higher education institutions in the Republic of Serbia, especially private ones, are located in Belgrade.

If we focus on higher education institutions for security, then according to the data from Table 1 we can notice that: 1) two state universities are directly targeted at the concrete security area: a) Defense University; and b) Criminal Police Academy for which a decision has been made to become a university – for public (internal) security, and 2) there is no one among private universities that is exclusively oriented at security education.

The fact that no private university in Belgrade is exclusively defined for security education certainly has several reasons, including the following: 1) the defense is immanent to the Army, and it is logical that the concentration of education for that segment is provided by the University of Defense (most of all, at the Military Academy); 2) public (internal) security has been strictly related to the Criminal Police Academy for a long time, which has grown into a university; and 3) there is a Faculty of Security at the Belgrade University, which, although it changed its name (Faculty of Defense and Protection, Faculty of Civil Protection) and programs, still has the longest tradition.

However, although there is no private universitiy exclusively focused on security education, some universities have: 1) faculties that have security in their name and 2) faculties under another name, on which the course (program) is security. Of the eight universities in Belgrade, there are three faculties with study programs on security (Table 2).

***Tabela 2**. Privatni univerziteti i fakulteti u Beogradu sa studijskim programom za bezbednost*

No	UNIVERSITY	FAKULTY	NOTE
1.	John Nesbitt (Megatrend)	Faculty of Law, Public Administration and Security	
2.	Union	Faculty of Law and Business Studies “Dr. Lazar Vrkatić” (in Novi Sad)	Course: Security and Criminalistics
3.	UNION – Nikola Tesla	Faculty of Diplomacy and Security	
		Faculty of International Politics and Security	
		Faculty of Business Studies and Law	Course: Security

Source: websites of the above universities

Na Univerzitetu “Dzon Nezbit” (bivši “Megatrend”, sa tendencijom da to ime vrati) postoji *Fakultet za pravo, javnu upravu i bezbednost*. Studijski program Pravo, javna uprava i bezbednost izučava se na sva tri nivoa: osnovne akademske studije (OAS), master akademske (MAS) studije i doktorske akademske studije (DAS). At the University of "John Nesbitt" (formerly "Megatrend", with the tendency to return this name), there is a Faculty of Law, Public Administration and Security. The law study program, public administration and security is taught at all three levels: basic academic studies (BAS), Master Academic (MAS) studies and doctoral academic studies (DAS).

At the University "Union" there is the Faculty of Law and Business Studies "Dr. Lazar Vrkatić" (with headquarters in Novi Sad), where the study program Security and Criminalistics at the BAS and MAS is being studied.

Na Univerzitetu "UNION – Nikola Tesla" postoje tri fakulteta na kojima se izučava studijski program bezbednost: 1) *Fakultet za diplomatiju i bezbednost*, na OAS sa studijskim programom Korporativna bezbednost na MAS; 2) *Fakultet za medjunarodne odnose i bezbednost,* na OAS i MAS sa najavom i na DAS i 3) *Fakultet za poslovne studije i pravo, sa smerom – Bezbednost,* na OAS i studijskim programom Međunarodna bezbednost na MAS. At the University "UNION - Nikola Tesla" there are three faculties studying the security program: 1) *Faculty of Diplomacy and Security*, at BAS with the study program Corporate Security at MAS; 2) *Faculty of International Relations and Security,* BAS and MAS with announcement for DAS; and 3) *Faculty of Business Studies and Law*, with the course - Security, at BAS and study program International Security at MAS.

STUDY PROGRAMES OF EDUCATION FOR SECURITY

According to the Law on Higher Education, the Study Program is a set of compulsory and elective study areas, that is, subjects with a framework content, whose mastery ensures the necessary knowledge and skills for acquiring a degree of appropriate level and type of study [*Law on Higher Education, 2017, Article 33*] . In addition, 1) *types of studies* are: a) academic and b) professional [Law, Article 34] and 2) *degrees* of study are: a) first (basic academic, basic vocational and basic specialist); b) Others (Master of Academic, Master Vocational and Specialist Academic) and v) Third - Academic Studies [*Law, Art. 35*].

Security is an extremely broad field of study for which it is not easy to accurately and specifically identify the field of education as a material for selecting the necessary subjects for mastering this knowledge. Namely, it is well known that security of science has long been denied identity, precisely because it is difficult to explicitly determine the subject of these sciences. This is because the subjects of security science, are at the same time the subjects of sociology, political science, legal science, psychology and other scientific fields. Apart from the subject, it is difficult to determine the method of security science, which should not to be proven.

In theory, security is spreading in several levels or in the security sector. The Copenhagen School of Security, ie its leading professor, Beri Buzan, identified those security sectors as: military, political, economic, social and environmental [*Pol D.Vilijams, 2012*].

From a practical point of view, if we focus on national security, we can speak about the external and internal security component [Stajić, 2013], which are viewed together as integral security of the country. To those security components we increasingly, rightly, add private and corporate security, as areas of practical activity that require scientific-theoretical design and study, ie education.

In accordance with the above, state and private higher education institutions act differently in the selection of study programs of security. In analyzing these commitments, targeted and for the reason, we will omit the University of Defense and the Criminal Police Academy.

Faculty of Security, University of Belgrade

The Faculty of Security of the University of Belgrade (State University), after decades of adjustment since its founding, has been stabilized in a very wide scope of security and tangential science fields, whose basic concept of BAS is expressed by the following: The concept of a basic academic studies program contributes to the development of civil society in terms of security (general, national, individual), protection (environment and population from natural disasters and chemical accidents, health and social, defense against contemporary forms of endangering and managing human and social resources with a focus on interdisciplinary approach. *[http://www.fb.bg.ac.rs/index.php?option=com_content&task=view&id=53&Itemid=360*].

In such a wide-ranging study of security at the BAS, called Security Studies, a large set of subjects was identified. The total number of cases in four years in BAS is 43, counting the final work (35 obligatory and 8 elective).

In addition to this, in addition to compulsory subjects at the BAS, elective courses are also being taught, while candidates are offered 32 elective subjects in four groups of subjects: security studies; studies of human and social resources management; civil protection and environmental protection studies and defense studies.

[http://www.fb.bg.ac.rs/index.php?option=com_content&task=view&id=53&Itemid=360].

I YEAR OF STUDY

No	TP[1]	SUBJECT	Sem.	No of classes		ESPB[2]
				Total	Per week	
1.	AO	Sociology	II	60	3+1	6
2.	TM	Basics of security	I	60	3+1	7
3.	AO	Legal basics of security	I	60	3+1	7
4.	AO	Basics of ecology	I	60	3+1	7
5.	AO	Psychology	I	60	3+1	5
6.	TM	Theories of conflict	I	60	3+1	6
7.	TM	Introduction to management	II	45	2+1	5
8.	AO	Introduction to security study	II	60	3+1	6
9.	AO	Ethics	II	45	2+1	5
10.	SA	English I	I i II	90	2+1; 2+1	6
		TOTAL:		600	20	60

II YEAR OF STUDY

No	TP[1]	SUBJECT	Sem.	No of classes		ESPB[2]
				total	Per week	
1.	NS	Regional geography	III	60	3+1	7
2.	NS	Political system	III	60	3+1	5
3.	TM	Systems of security	III	60	3+1	7
4.	NS	International relations	III	60	3+1	5
5.	NS	Basics of geopolitics	III	60	3+1	5
6.	NS	Information science	IV	60	2+1	5

7.	TM	Systems of protection and saving	IV	60	3+1	7
8.	AO	Theory and organization of education	IV	45	2+1	6
9	TM	Defense systems	IV	60	3+1	5
10.	SA	English II	III i IV	90	2+1; 2+1	6
		TOTAL:		**600**	**20**	**60**

III YEAR OF STUDY

No	**TP[1]**	**SUBJECT**	**Sem.**	**No of classes**		**ESPB[2]**
				total	Per week	
1.	TM	Management of human and social resources	V	60	3+1	5
2.	NS	Criminal law	V	60	3+1	5
3.	NS	System of civil defense	V	60	3+1	6
4.	NS	Criminology	V	60	3+1	6
5.	SA	Civil protection	V	60	3+1	6
6.	TM	Modern history of Serbia	VI	60	3+1	4
7.	SA	Elective subject 1	VI	60	3+1	6
8.	SA	Elective subject 2	VI	60	3+1	6
9.	SA	Elective subject 3	VI	60	3+1	6
10.	SA	Elective subject 4	VI	60	3+1	6
11.	SA	Professional practice	V i VI			4
		TOTAL:		600	20	60

IV YEAR OF STUDY

No	**TP[1]**	**SUBJECT**	**Sem.**	**No of classes**		**ESPB[2]**
				total	**Per week**	
1.	NS	International public law	VII	60	3+1	6
2.	NS	Civil-military relations	VII	60	3+1	5

3.	NS	Environment protection	VII	60	3+1	6
4.	NS	Security management	VII	60	3+1	6
5.	TM	Methodology of scientific research	VII	60	3+1	5
6.	SA	Crisis management	VIII	60	3+1	5
7.	SA	Elective subject 5	VIII	60	3+1	5
8.	SA	Elective subject 6	VIII	60	3+1	5
9.	SA	Elective subject 7	VIII	60	3+1	5
10.	SA	Elective subject 8	VIII	60	3+1	5
11.	SA	Professional practice	VII i VIII	60	3+1	5
12.	SA	Final paper	VIII	60	3+1	5
		TOTAL:		**600**	**20**	**60**

Na MAS postoje dva smera: 1) Studije nauka bezbednosti i 2) Studije upravljanja rizicima od elementarnih i drugih nepogoda. There are two courses at MAS: 1) Safety Science Studies; and 2) Risk Management Studies of Elementary and Other Disasters. [*http://www.fb.bg.ac.rs/index.php?option=com_content&task=view&id=62&Itemid=350].*

Na DAS je samo jedan smer – Studije nauka bezbednosti ciji su predmeti prikazani u sledecoj tabeli. DAS has only one course - Studies of Security Science whose subjects are shown in the following table.

SUBJECTS AT DOCTORAL STUDIES

No	**TP**	**PREDMET**	**Sem.**	**No of classes**		**ESPB**
				total	**Per week**	
1.	O	Studies of modern and safety aspects	I	45	3	5
2.	O	Modern theoretical approaches to studying security	I	45	3	4
3.	I	Elective modul – Security	I	60	4	8

4.	I	Study and research work	I	150	10	13
5.	I	Elective modul - Defense	II	60	4	8
6.	I	Elective Modul – Management of human and social resources	II	60	4	8
7.	I	Elective modul –Civil and environmental protection	II	60	4	8
8.	O	Study and research work	II	120	8	6
TOTAL:				**600**	**40**	**60**
II YEAR						
1.	O	Methodology of research of security cases	III	60	4	6
2.	I	Study and research work	III	240	16	24
3.	O	Special elective course	III	75	5	6
4.	O	Development and defense of the PhD topic project	IV	225	15	24
TOTAL:				**600**	**40**	**60**
III YEAR						
1.	O	Study research work and preparation of doctoral dissertation	V i VI	600	40	60
TOTAL:				**600**	**40**	**60**
TOTAL:				**1800**	**120**	**180**
ELECTIVE MODUL SUBJECTS						
1.	I	Studies of security policy and security strategy	I	60	4	8
2.	I	Communication aspects of security	I	60	4	8
3.	I	Modern systems of collective defense	II	60	4	8
4.	I	Geopolitic aspects of national defense	II	60	4	8
5.	I	Management of human resources and management of total quality	II	60	4	8
6.	I	Management of education in the security area	II	60	4	8
7.	I	Management of risks and crisis in environment	II	60	4	8
8.	I	Development, conflicts and environment	II	60	4	8

Source: http://www.fb.bg.ac.rs/index.php?option=com_content&task=view&id=71&Itemid=367

From the data provided for the Faculty of Security, obviously, it can be concluded that security has been affected very widely, involving: 1) general security; 2) defense; 3) civil protection and environmental protection; and 4) to some extent internal security (criminalistics and criminology). The fact is that at the Faculty of Security there is no private or corporate security.

Private institutions of higher education

Private higher education institutions (the three listed universities), at the faculties that are in their composition, involve a different study of security, which will be illustrated in the following examples.

Faculty of Diplomacy and Security

The Faculty of Diplomacy and Security has developed BAS and MAS announcing also organization of DAS. [http://www.diplomatija.com/].

At the basic studies, which last for three years, there is a study program Diplomacy and Security. In the mentioned study program, a total of 39 subjects are studied, with only four in the group of the so called security subjects: Security systems; International Security; Intelligence and Security Services and Security Skills. [http://www.diplomatija.com/studijski-program/osnovne-studije/].

Master studies include two study programs: 1) Diplomacy and Security, and 2) Corporate Security [http://www.diplomatija.com/].

Master studies Diplomacy and security last for two years. In these studies, compulsory and elective subjects are studied. The total number of subjects is 21 (13 compulsory and 8 elective). Typical security items are mainly in the group of elective subjects (modern security integration and military diplomacy, national security strategy, civil security, Serbia's security system), while only two in the compulsory subjects group (security policy and security skills). [*http://www.diplomatija.com/studijski-program/master-studije-diplomatija-i-bezbednost/].*

Master Studies Corporate Security last for two years. In these studies, compulsory and elective subjects are studied. The total number of subjects is 13 (7 compulsory and 6 elective). In this study program, most subjects focus on corporate security. Practically, all subjects, other than the Methodology of Political Science, are in the domain of corporate security and tangential areas: 1) Theory of Corporate Security; Corporate Security Management; Modern Economy and Security; Physical-technical protection; Industrial safety; Ecological safety; Technical and technological accidents; Industrial Safety Management; Civil Security; Endangering corporate security; Security Skills and Contemporary Corporate Security Systems. [*http://www.diplomatija.com/studijski-program/master-studije-korporativna-bezbednost/*].

Faculty of International Politics and Security

The Faculty of International Politics and Security of the University "UNION-Nikola Tesla" educates students on BAS and MAS, with the announcement of DAS. At the BAS there are 44 subjects classified as compulsory and elective, including the final paper. Out of 44 subjects, only eight are in the group of "pure" security, so only one (Security Basis) is obligatory, while the other seven are in the group of elective subjects. Electoral subjects include: Terrorism and organized crime; Security and crisis management; Security system of the Republic of Serbia; Intelligence and security services; Security and media; EU Common Foreign and Security Policy and Contemporary Challenges and Threats to International Security. [*http://www.fpb.edu.rs/planovi/oasfmpb.pdf].*

Master studies are organized as a program International Politics and Security and last for one year. 9 compulsory and elective subjects, including final paper, are taught at MAS. A set of security subjects, all of which are elective, include: Modern security systems; Religious fundamentalism and extremism; Analyzes of political and security phenomena; Globalization and Security and Strategic Governance in Political and Security Processes.

[http://www.fpb.edu.rs/planovi/masfmpb.pdf].

In accordance with the above data, it can be concluded that the Faculty of International Politics and Security, primarily, is focused on studying international politics, with security as incidental phenomenon. On the other hand, this faculty is not program-oriented at all towards private and corporate security.

Faculty of Law, Public Administration and Security – FACULTY OF LAW

Based on the request of the Faculty of Law, Public Administration and Security of the University "John Nesbitt" in Belgrade, dated 8 April 2016, The Ministry of Science and Technology Development of the Government of the Republic of Serbia has changed the name of the former Faculty of Law, Public Administration and Security in the FACULTY OF LAW. At the Faculty of Law, security is taught at BAS, MAS and DAS. On BAS - Law and Security, and on MAS and DAS / - Law, Public Administration and Security

[*http://naisbitt.edu.rs/2016/07/promena-imena-fakulteta-za-pravo-javnu-upravu-bezbednost/].*

The BAS Security module is very interesting. The Security module includes 36 obligatory and elective subjects, whereby: 1) objects from "pure" security issues appear only in the third year of studies and are mostly in the group of elective subjects. Obligatory security subjects are: Security systems; Criminology; Security law; Ecological safety; Security analysis and Methods and techniques of security organization and operation. The group of elective subjects are: Social Crises and Conflict; Organized criminal; Criminalistics; Terrorism; International Security Organizations and Corporate Security. [*http://pf.naisbitt.edu.rs/osnovne-studije/]*

Master academic studies are a bit complicated. Namely, MAS under the name Law, public administration and security has moduls of Law, Public Administration and Security, then the module Law has sub-modules. The Security module does not have submodules. Three compulsory subjects are studied on all modules: Methodology of scientific research; Public Administration and Management and Special Administrative Law. On the Security module, the student chooses three of the following six electives: Modern Security Systems; Common EU foreign and security policy; Contemporary Criminal Theories; Crisis Management; Environmental Safety and Security Analysis. [*http://pf.naisbitt.edu.rs/master-studije/].*

Study program of doctoral academic studies - *Law studies, public administration and security* within the field of social sciences and humanities is accredited by the Commission for Accreditation and Quality Assurance, a certificate on the accreditation of the study program of doctoral studies number: 612-00-02669 / 2013-04 of 23/05/2014. Doctoral academic studies last for three years, 180 ESPB points, and can be entered by a person who has completed basic academic and master academic studies of law or a study of political-legal, legal-business, security-legal and other related subjects with at least 300 ESPB, with a score of at least 8 (eight) at basic studies and with the knowledge of a foreign language in a degree that enables him to use foreign literature in that language. *[http://pf.naisbitt.edu.rs/doktorske-studije/*]

There are two mandatory and three out of five electives in the DAS Security module. Mandatory subjects are: Methodology of scientific research and Theory of state and politics. Elective courses are: The current problem of international law; Modern security theories; Comparative public (security) policies; International Criminal Law and Criminology with panology and victimology. [*http://pf.naisbitt.edu.rs/doktorske-studije/].*

From the above data on the Law Faculty of the University "John Nesbitt" it can be concluded that the study program Security is subordinate to the study programs Law and Public Administration, and that it is quite extensive in regard to its subjects. Corporate security is studied only within a single subject at the BAS.

Faculty of Business Studies and Law

The Integrated Educational System for Social and Primary Sciences (IES) from Belgrade is the founder of the Faculty of Business Studies and Law (FPSP) - Belgrade, Faculty of Strategic and Operational Management (FSOM) - Belgrade, UŠĆE High School in Belgrade, elementary "Kosta Vujic" school in Zemun, Pre-school establishments "Kosta Vujic" in Zemun and Scientific Research Center (SRC) from Belgrade. All educational institutions are accredited, have a license to work from the competent ministry and operate within the Integrated IES education system. [*http://www.fpsp.edu.rs/wp-content/uploads/2017/02/Informator_2017.pdf].*

At the Faculty of Business Studies and Law there is a course Security, which is being studied at BAS and MAS. At the BAS as a study program Security, and at MAS as International Security.

The Security Study program at BAS, predominantly includes security subjects, as well as subjects of tangential areas (law, economics, management ...), which are grouped into mandatory (80%) and electoral (20%) subjects. The studies last for four years and include 32 subjects, including final paper. Typical subjects from the security domain are: Basics of Security; Security systems; Criminology with social palliology; Corporate Security; Protection of information security; Crisis Management; Security analysis; Intelligence and security services; Security Management; Security in emergency situations; Environmental Management Systems; Managing Change and Conflict; Detective activity; Criminalistics and Terrorism and Organized Crime. Thus, 50% of the subjects in the Security study program are directly from the field of security. [*http://www.fpsp.edu.rs/wp-content/uploads/2017/02/Informator_2017.pdf].*

At the MAS there is the study program International Security and it lasts for one year. The program includes seven subjects of compulsory and elective character, including master paper: Methodology of Scientific Research Work; Modern security theories; Modern diplomacy or Conflict and Peace Strategy; The Organization of International Security or the Contemporary Foreign and Security Policy; External and security policy of the EU and the SIR in international security. [*http://www.fpsp.edu.rs/wp-content/uploads/2017/02/Informator_2017.pdf].*

Based on the information provided for the Faculty of Business and Law, it can be concluded that the study program Security is extremely represented and that the security sector is more complete than at any other private faculty mentioned above. Corporate security and detective activity are represented by one subject each.

THE REASONS FOR FOCUS ON CORPORATIVE SECURITY

It is a fact that security study programs had been a "privilege" of state-run higher education institutions for many years. The education of private higher education institutions, in accordance with the Law on Higher Education, is not limited by the choice of a study program. However, despite this fact, private higher education institutions have opted for other study programs, in the sphere of socio-humanistic, natural-mathematical and technical-technological educational-scientific fields. However, the "market game" (a surplus of non-registered students at state faculties) has also prompted private higher education institutions to develop security study programs over time. In addition, the study program security, most often, is related to some activity (diplomacy, international politics, law), but does not exist independently. In this regard, private higher education institutions have acted pragmatically, that is, in the areas of the core activity that added security, they did it extensively, trying to attract the young population.

Corporate security is only in a sporadic way, primarily as a subject, represented at private higher education institutions, with the exception of the Faculty of Diplomacy and Security, where MAS Corporate Security exists. It can be said that this faculty recognized the need imposed by the practice.

Namely, the transition of the state to private property, as a basic form, has opened up huge space for the need for educated personnel specializing in corporate security. Certainly, state-owned companies require a highly educated corporate security personnel. This is also supported by the opening of an increasing number of foreign companies in our country. The fact is that security jobs and security (corporate security) in these companies are mostly performed by persons who have completed the state security faculty faculty (Military Academy, Criminal Police Academy or the Faculty of Security).

The special reason for focusing of private higher education institutions on corporate security lies in the fact that it has come or will quickly come to saturation of the country's market with highly educated general security personnel, while the need for highly educated personnel in the field of corporate security will continue to grow.

It is not unknown, although it is not popular, nor is that something that should be praised, that a large number of highly educated people in our country, looking for a secure and better paid job, are going abroad. It is hard to imagine that when educated for general security and defense, they will be tempting in other countries. However, higher education for corporate security, which in principle does not know the boundaries, offers quality that can have more propulsion abroad.

At the end, not by importance, it should be noted that in modern conditions of business there is a so-called corporate social responsibility, which is based on the introduction and implementation of various standards, among which are standards that affect the security of corporations. Herewith we mention two standards: 1) Standard SA 800 (international standard for improvement of working conditions), which is based on nine elements, including the Health and Safety element, and 2) ISO 1400 standard - environmental management, as a special form of corporate social responsibility. [Ćeha, *2011*].

CONCLUSION

Security is the basic precondition for survival and development of the human community. National security is the basic function of each state, which is organized as a normative, functionally and organizationally determined system. In every national system, education is particularly important.

Security education in the Republic of Serbia has long been a privilege of state higher education institutions, such as the Faculty of Security, the Military Academy (now the University of Defense) and the Criminal Police Academy. For one or two decades, private higher education institutions have become more numerous than state-owned ones.

At the beginning, private higher education institutions were more focused on study programs of social-humanistic (without security), natural-mathematical and technical-technological field. However, in the last decade more and more of these institutions opt for the security study program.

The security study program at private higher education institutions is primarily related to another activity, such as diplomacy, international politics, law, and rarely appears independently. On the other hand, the study program security is initially set up very extensively, which has its justifications in the efforts of private higher education institutions to attract "surplus" of youth population that have not enrolled in state faculties.

Corporate security is in a fragmented way (in the form of subjects) present at private higher education institutions, with the exception of the Faculty of Diplomacy and Security with Master Studies in Corporate Security.

Although it has been very popular among young people for decades, the Security program, primarily in state and private higher education institutions, has educated a large number of personnel, which will inevitably lead to saturation of the market. This is one of the reasons why private higher education institutions are focusing on corporate security. However, other reasons are more important than the foregoing and are reflected in: 1) the fact of the transfer of state to private property, 2) the legal basis for corporate security regulation, 3) international and domestic standards of corporate business, in which corporate security standards are applied; 4) increasing foreign investment and opening foreign companies in Serbia; and 5) relative propulsion of higher education for corporate security in international terms.

Corporate security as a study program of higher education institutions is a challenge. As so many times before, it will be shown that – whoever starts first, will have the greatest benefits.

REFERENCES

1. *Zakon o visokom obrazovanju*, „Službeni glasnik RS", br. 88/2017.

2. Keković, Zoran, (2011), *Sistemi bezbednosti,* Fakultet bezbednosti, Beograd.

3. Mijalković, Saša, (2011), *Nacionalna bezbednost,* Kriminalističko-policijska akademija, Beograd.

4. Stajić, Ljubomir, (2013), *Osnovi sistema bezbednosti*, Pravni fakultet, Novi Sad.

5. *Strategija nacionalne bezbednosti Republike Srbije*, „Službeni glasnik RS", br. 88/09.

6. Trivan, Dragan, (2012), *Korporativna bezbednost*, Studio Dosije, Beograd.

7. *Uvod u studije bezbednosti*, priredio Pol D. Vilijams, (2012), Službeni glasnik i Fakultet bezbednosti, Beograd.

8. Forca, Božidar, Intervju on-line magazinu *Odbrana i bezbednost*, dostupno na: https://magazin.istrazivackicentarob.com/2017/09/08/o-vojnoj-neutralnosti-srbije-od-ljubavi-do-mrznje-samo-interes-nas-deli/ (30.11.2017).

9. Forca, Božidar**,** Sekulović, Dragoljub, (2017) *Identifikacija problema savremenih strategija bezbednosti: studija slučaja – Republika Srbija*, Zbornik radova sa nacionalnog naučnog skupa „Savremeni problemi strategije i strategijskog menadžmenta", Fakultet za poslovne studije i pravo, Beograd.

10. Ćeha, Milenko, (2011) *Uloga korporativne dru[tvene odgovrnosti u savremenom poslovanju u Srbiji,* doktorska disertacija, Univeryitet Singidunum, Beograd.

11. http://www.edufair.rs/fakulteti/ (30.11.2017).

12. http://www.fb.bg.ac.rs/index.php?option=com_content&task=view&id=53&Itemid=360 (30.11.2017).

13. http://www.fb.bg.ac.rs/index.php?option=com_content&task=view&id=62&Itemid=350. (30.11.2017).

14. http://www.fb.bg.ac.rs/index.php?option=com_content&task=view&id=71&Itemid=367 (30.11.2017).

15. http://www.diplomatija.com (29.11.2017).

16. http://www.diplomatija.com/studijski-program/osnovne-studije/ (29.11.2017).

17. http://www.diplomatija.com/studijski-program/master-studije-diplomatija-i-bezbednost/. (29.11.2017).

18. http://www.fpb.edu.rs/planovi/oasfmpb.pdf (30.11.2017).

19. http://www.fpb.edu.rs/planovi/masfmpb.pdf. (30.11.2017)

20. http://naisbitt.edu.rs/2016/07/promena-imena-fakulteta-za-pravo-javnu-upravu-bezbednost/. (30.11.2017)

21. http://pf.naisbitt.edu.rs/osnovne-studije/ (30.11.2017).

22. http://pf.naisbitt.edu.rs/master-studije/. (30.11.2017)

23. http://pf.naisbitt.edu.rs/doktorske-studije/. (30.11.2017)

24. http://www.fpsp.edu.rs/wp-content/uploads/2017/02/Informator_2017.pdf. (01.12.2017)

UDC 007:004.56

CORPORATE SECURITY IN THE CYBER ENVIRONMENT

***Tanja Kaurin*[1], *Zdravko Skakavac*[2]**

[1] Faculty of Law and Business Studies dr Lazar Vrkatić
[2] Faculty of Law and Business Studies dr Lazar Vrkatić

The cyber environment is in continuous expansion. New technologies and trends affect the widespread and new threats. With vague borders, hidden users, it is globally present, and is a huge challenge for companies. The benefits that it offers always bring about challenges, risks, and threats that sometimes are difficult to deal with. Corporate security has been a hot topic practically since the beginning of the use of information technology, and it depends on the technical component, organizational aspects of corporations and applied knowledge. Violation of any segment in the security chain, even if unintentionally due to ignorance, unreasonableness or misunderstanding, can lead to a disruption of the production process and damage to business (financial losses, loss of reputation, etc.). When it comes to corporate security in cyberspace, focus is on cyber threats. It should be kept in mind that these are high profile and high impact attacks by organized, sophisticated and committed cyber criminals. Clearly, a critical part of cybersecurity is actually a human factor, and it is necessary to develop a positive security culture. The role of the state in corporate security is indisputable, especially in the segments of the judiciary, security services, education, the development of IT sectors and state bodies and organizations.

INTRODUCTION

In the last two decades, cyber space has become a widely accepted arena for wider and faster communication, an economic sphere that simultaneously intertwines with the social lives of individuals. The online presence of individuals, companies and governments as a positive side and the true core of the technology era, is widely used as a place to promote interest through malicious activity. The latest analysis by Microsoft and independent analytical houses in the area of information security and cyber attacks show that companies and individual users worldwide are more vulnerable than ever. The cyber threats are ubiquitous - from hacking attacks to organized criminal groups over sophisticated abuse and financial scams of companies, government organizations, social networks and individuals. This global problem affects more than one million people every day, and every seven minutes a company becomes a victim of cyber-fraud. Today, there is virtually no area without information technology (IT): financial transactions, industrial processes, scientific research, education, health, transport, public administration, national defense and security of the country, the exercise of personal rights of citizens, and more. The exceptional possibilities of IT application have significantly contributed to the change in the performance of jobs and people's lives. This is primarily based on the fact that almost all human activities require accurate, complete and timely information, which justifies the application of IT. In other words, IT has greatly expanded human capabilities in the arena of collecting, storing, processing, using and presenting information. [Kaurin & Skakavac, 2017]. A brand new level of sophistication and technology development faces companies with new security threats. Cloud technology, crypto-development, and IoT (Internet of Things) are just some of the reasons for the increased number of cyber threats and their diversity. The main features are their complexity and automation, and the higher level of concealment and professionalism. Risks range from equipment failure, errors in programs and procedures, human error, to the deliberate destruction or alteration of data, damage and disabling of the equipment, misuse of information, intellectual property theft and block of the performance of information systems, it becomes extremely difficult to fight with traditional methods.

In performing tasks, IT is characterized by: availability, volume, communicativeness, economy, speed, precision, reliability and more. The use of IT significantly increases and expands human capabilities, which has led to an extremely large and wide application. The widespread use and accessibility, on the other hand, has led to the misuse of ICTs. Abuse is reflected in numerous and varied potential threats and dangers that endanger corporate security. [Anucojić, 2010]

Abuse of IT, which has the character of criminal activities, imposes the need for an adequate security system. This system should be well-designed, comprehensive, detailed, with security and control mechanisms, with precisely defined rights, responsibilities and sanctions for all categories of corporate environment entities.

The basic segments (security categories) of the security system, according to the ISO / IEC standard, are:

1. Risk assessment
2. Security Policy
3. Organizacija informacione bezbednosti (eng. *Organization of information security*),
4. Asset Classification and Control
5. Human resources security
6. Physical and Environmental Security),
7. Communications and Operations Management
8. Access Control
9. Information systems acquisition, development and maintenance
10. Information security incident management
11. Business Continuity Management
12. Compliance

Each of the above segments is a special and very complex whole, but they are all in very strong correlation. Their content is closely related to the functions of the corporate system in question, its significance and degree of confidentiality of business and data.

CYBER THREAT LANDSCAPE AND SECURITY

In a modern, digitally connected world, threats to the cyber environment come from unexpected sources and unpredictable directions. Not only the number, but the scale and severity of cyber threats are developing at a dramatic speed. We are witnessing the everyday occurrences of malicious innovative methods whose development and distribution are conducive to precisely the specificity of cyber space. With growth in target values, sophistication of protection mechanisms also increases, but attacks also change form, function, target group and are far advanced compared to those of a few years ago. The number of highly profiled attacks on large companies such as Target, AOL and eBay illustrate the ambition of many attackers. According to the report for 2016, it is estimated that the number of data endangered by cyber attacks has risen to over half a billion [Symantec, 2017]. The incidence of different types of digital data such as: financial transactions, information about products or projects, personal user data and other personal information or information that is an intellectual property make cyber space an important source of rich, highly valuable information. The motives of these attacks are no longer purely financial in nature, but all of them combine social and political aspects. The number of threats is higher than ever with an increase in frequency and severity. In addition to the seriousness of cyber security, the fact that NATO officially recognized cyberspace as the fifth domain of war is the fact that the need to react with conventional weapons in case of strong cyber attacks, and the global strategy of the EU's foreign and security policy defined the cyber security issue as one of the five priorities for the security of the Union's foreign policy.

To clarify this term, it is necessary to first of all clarify the term Cyberspace. Cyberspace is one of the most used computer concepts, and is descriptively presented as a virtual computing environment. According to the Merriam Webster dictionary definition, it is the online world of computer networks and the Internet. The Cambrige dictionary in the British English version explains cyberspace as an internet-free imaginary space where people can get information and get information on any topic, while in the American English version it is an electronic system that allows computer users around the world to communicate with each other or access information for any purpose. Technopedia gives a more detailed explanation of this term: Cyberspace refers to the virtual world of computers, or more specifically, an electronic medium used to form a global computer network to facilitate online communication. It means a large computing network composed of many computer networks around the world that use the TCP / IP protocol to help them to communicate and exchange data. This explanation is similar to that provided by the National Institute of Standards and Technology (NIST): A global domain within an information environment consisting of an interconnected network of information systems including the Internet, telecommunication networks, computer systems, and embedded processors and controllers. The main feature of Cyberspace is the interactive and virtual environment for a wide range of participants that allows users to exchange information / ideas, communicate, entertain, participate in discussions or social forums, connect business and similar. According to many IT experts,, cyberspace has gained popularity as a medium for social interaction, and not technical realization and implementation [Kaurin & Skakavac, 2017].

When we want to consider cyber security by insight into literature, we notice that the notion of information security is equally represented. Whether and to what extent these two concepts overlap largely depends on the author's interpretation.

Von Solms and van Niekerk believe that information and cyber security are two different concepts that have only certain areas of overlap, and that they are not analogous terms. Information security considers protection of data against possible damage caused by various threats and vulnerabilities. Cyber Security, on the other hand, is interpreted as protection not only of cyber space but also the protection of those operating in cyberspace as well as the protection of their property that can be accessed through cyber space [Von Solms & Niekerk, 2013].

NIST defines cyber security as - The ability to protect cyber space from cyber attacks, and information security as the protection of information and information systems from unauthorized access, use, detection, disturbance, modification or destruction to ensure confidentiality, integrity and accessibility. The International Telecommunications Union (ITU) defines cyber security as follows: Cyber Security is a set of tools, policies, security concepts, security guarantees, guidelines, risk management approaches, actions, training, best practices, security and technologies that can be used for protection of cyber environment, organization and users' funds. Organization and resources of users including connected computer devices, personnel, infrastructure, applications, services, telecommunication systems, as well as total transfers and / or stored data in a cyber environment. In the official documents of the Republic of Serbia, the term "information security" is used, while “cyber security” is more present in international documents [Kaurin & Skakavac, 2017].

When it comes to security in general, and in particular security in the cyber environment, it is important to emphasize that security must not be perceived as a finished product or a final state. Security is the process of maintaining a level of acceptable risk that implies the application of different products and services, respecting procedures and rules, educating people, and constantly monitoring developments in this area and spreading awareness. The basic concept of security, known as the CIA (Confidentiality, Integrity, Availability) triad, refers to respecting the three fundamental principles of information security to be applied regardless of the way of storage (digital or traditional):

- Confidentiality. It can be said that it is roughly equivalent to privacy. It implies protection of data from unauthorized access and requires measures to ensure that only authorized persons can access information.
- Integrity. This means protecting data from unauthorized persons or processes. Integrity is maintained when data remains unchanged during storage, transfer, and use.
- Availability. This implies the possibility of timely access to data by authorized persons. Availability is possible when all information system components work properly.

On the basis of the above, it is noticeable that the CIA triad is, above all, the protection of information, and that the protection of infrastructure as well as people involved in the process itself should be considered. If the CIA triad is viewed as security of information, the next category of technology-based infrastructure definitely belongs to the category of information communication technologies, and, if there is a need for it, it can be distinguished as IT security. In this case IT security would be considered to protect a wide range of technologies based on computers, networks and data storage. There is a need to protect people and society that could then get prefix cyber and call it cyber security. This would actually refer to IT security and information security, but with the emphasis on the cyber environment. The foregoing means that cyber security would be the protection of persons, societies and nations, including their informational and informal environment. It would be realized through tools, security concepts, guidelines, risk management, application of best practices and adequate technologies to protect the interest of an individual, society or nation [Skopik, 2017]. In a wider context, Cyber Security overlaps with several other aspects of security [Sutton, 2017]:

- Information security, which deals with the protection of confidentiality, integrity and accessibility in all areas of information, not just those in cyberspace.
- Application security, which deals with the control and monitoring of applications.
- Network security, which deals with the provision of network protection, within the organization, between organizations and between the organization and its users.
- Internet security, which deals with protecting the availability and reliability of Internet services at the organization level and protecting individual users both at work and in their private environment.
- Protection of critical information infrastructure covering the aspects of cyber security of elements of critical information infrastructure in the country.

The aim of cyber security is to prevent, detect and respond to cyber incidents and attacks as well as alleviating cyber threats. Unlike physical threats, in a virtual environment, threats remain easier and anonymous. Most definitions of cyber attacks focus only on information security or ICT security, but it rarely deals with the holistic nature of these types of attacks. Strictly speaking, the cyber attack refers to an attack carried out through ICT and compromises the cyber security of individuals, companies or states. Cyber attacks can cause various consequences, such as access punching, data exfiltration (unauthorized download), identity theft, fraud, intellectual property theft, denial of service (DoS), or malware infection, but it should be noted that there it does not mean that every cyber attack might potentially escalate into a serious one with dramatic consequences.

Depending on the type of threats, their impact on the victim may be short-term or long-term. The short-term impact relates to the day-to-day activities of individual end-users (for example, their ability to access up-to-date information and perform financial transactions, such as cash withdrawals at ATMs). Obstructing everyday activities of the company can lead to significant financial losses. A long-term impact may be a national security breakthrough (Wikileaks example). Social dissatisfaction and unrest (for example, losing confidence in the government, even if the actual damage caused by cyber criminal activity was minimal). The actors of threats can be individuals or groups who commit or intend to commit cyber attack. Cyber security threats can be divided into sophisticated and unsophisticated. They include countries, cybercriminals, criminal organizations, hackers, extremists and insiders. It is important to emphasize that these categories are not mutually exclusive.

Companies are often the target of an attack because the cost-effectiveness of the attack, if successful, is high. Although the essence is the same it is possible to notice two types of attacks. The first is when the real goal is not the company itself but something that it owns, such as a customer database and credit card information; something that the company has developed, such as a new product or service; something that the company plans, such as the takeover of a competing organization; or simply details of the financial position of the organization. The other is when the target is a specific company or its business and in this case the intention of the attacker is to cause immediate financial or reputational damage. When financial criminals attack, the goal is profit and their target are financial institutions and population. This category of criminals can significantly vary in the level of knowledge and skills. There are criminals (groups) who have advanced levels of knowledge and also have professional equipment. At any moment they can offer their services to others at a certain price. This makes it possible to increase the number of cyber criminals because even less experienced or less equipped criminals can commit complex cyber attacks. It can be said that cybercriminal is a well organized, developed business with a developed underground market that also helps criminals with less knowledge and skills to engage in cybercrime activities. It is possible to attack credit card information and other relevant personal information as well as different types of "goods" that can be misused for personal financial gain. [Kaurin & Anucojić & Skakavac, 2017].

In an extremely dynamic IT environment that in itself represents a huge challenge to the security and economic viability of many companies, attention needs to be paid to new technologies that further complicate the problem of cyber security. Some of them are:

- Internet of Things – IoT,
- Big Data,

- Wireless technology
- Cryptocurrency

The Internet of Things is one of the most important technological trends with an impact on security. Devices connected via the Internet quickly found their way to consumers and companies in particular in sectors such as manufacturing, health, and entertainment. Considering that most companies are still struggling with the risks of the phenomenon bring your own device (BYOD), it is clear that IoT will additionally intensify a sufficiently serious situation. IoT greatly changes the virtual but real world, since with the increase in the number of devices the number of generated data grows. Big Data generated with an increasing amount of information from sensors, smart systems, entertainment devices and social media applications has a tendency of constant growth with the necessity of improving analytical techniques. The processing of Big Data, especially the merging of different databases, confronts two great challenges to privacy and safety.

Wireless technology and the use of wireless devices are another major risk. The increase in the use of wireless office equipment and access points increases the possibility of attacks on potentially targeted systems. In addition, it is possible to jeopardize the availability of the network by blocking authorized users.

Cryptocurrencies dramatically change the financial sector and cyber domains by enabling cyber attacks, especially ransomware. The virtual currency is difficult to track in classical cash flows, and it is precisely because of this trait that it is adequate for criminals. According to reports of all eminent ransomware companies, attacks had steadily increased in the number and amount of virtual money collected during 2016 and 2017, and although some industrial branches were more affected, data shows that no sector was spared. In the US and Western Europe, 20 percent of small businesses affected by the virus were forced to stop working because of data loss.

Obviously, the modern environment implies a completely different approach to security issues. The evolution of human behavior as a result of technological innovation has created unique opportunities for crime and abuse. Over the past three decades, the constant growth of new devices and applications resulted in the modification of traditional forms of criminal activity and the formation of completely new ones. Demolishing the borders and facilitating communication, regardless of the physical location, the Internet has actually made it possible for members of organized crime groups to virtually be present anywhere in the world. Unlike the off-line world where it is necessary to be physically present at the crime scene and where one crime can be committed at one time, cyber space has enabled the organization and attacks on a large number of victims, at the same time in a large number of different locations, without significant risk and effort to hide identity. [Kaurin & Skakavac, 2017].

THE ELEMENTS OF CORPORATIVE SECURITY

The term corporate security consists of the means, measures and activities designed to prevent or reduce the threat to material goods, the rights and lives of people, the environment, the state and society. In the IT domain, the term corporate security covers the protection of IT equipment, infrastructure, programs and data. Potential threats which may compromise information systems and data can be classified into the following categories: "Force Majeure" (earthquake, storm, flood ...); disadvantages (defects) in equipment and programs; human factor with an attribute of inadvertence; and human factor with an attribution od doing it on purpose [Kaurin & Anucojić, 2011].

The goals of corporate security are the prevention of endangering, detection of threats, acts in case of threats and the elimination of the consequences of endangering. In order to fulfill the set goals, protection must be planned, designed and implemented comprehensively, in a organized way, professionally and rationally. The starting points for the introduction of corporate security are the answers to the following questions: What to protect? From whom or from what to protect? Why protect? Protect with what? and How to protect? After considering the starting points, corporations often face the following problems:

- Cyber security is viewed as an intricate topic, and many individuals and smaller organizations feel that they do not possess the necessary knowledge or skills to understand or take the necessary actions to protect themselves from cyber attacks.
- Companies, regardless of size, often lack the human resources available to engage in this kind of business.
- Managers are not able to fully understand the need for adequate cyber security and its importance, and also fail to understand that the

data and information of an organization belong to them, and not to the IT sector.

Due to its seriousness, complexity and importance, the protection of information systems, and especially its legal aspect, has been the subject of studies, discussions and decisions of various national and international bodies and organizations for years, and the number of countries that have regulated this issue is constantly increasing. Starting from the basic goal of corporate security of information systems, to ensure and protect the integrity and availability of computer equipment, as well as the integrity, availability and secrecy of data and information, one could conclude that the current situation is not satisfactory and that there is still much to be done in this area. Governments of many countries, as well as numerous professional and commercial organizations, associations and institutions have invested and are making great efforts to solve the problem of corporate security of automated information systems. The EU's Single Digital Market Strategy clearly recognizes the importance of IT security for the functioning of the digital market. This strategy highlights the need to define technological standards that support the development of the digital market and service sector - including the necessary standards of IT security. The Action Plan for the establishment of a single digital market envisages the adoption of the Plan of Priority IT Standards. The strategy also opens the question of creating a contractual public-private partnership in the field of cybersecurity, which is dealt with by the Directive on the creation of a contractual public-private partnership for industrial research and innovation in cyber security.

Protection management is a very complex process regarding organization and necessary experts. Planning, realization and implementation of corporate security takes place simultaneously with the planning, implementation and functioning of the information system. It develops in parallel with the development of the information system and lasts longer than the information system itself (deadlines for storing data and information). Most of the systems of corporate security, especially in the planning and implementation, are realized by specialists in cooperation with equipment manufacturers and software makers. It can be said that key segments of protection management are: risk analysis, defining objects that need to be protected, detection of possible threats - dangers, identifying possible consequences, proposing measures of corporate security and defining corporate security policy [Kaurin & Anucojić, 2011].

Legal regulations. Corporate security is part of the legal system that relates to the prosecution of high-tech criminals. Due to differences in the rules applicable in the relevant legal process, as well as in the procedure itself, depending on the state in which it is being dealt with, there is a problem of jurisdiction that arises in situations where a criminal uses resources in one country for committing criminal acts in another, while he commits criminal offense in a third country. Such action requires international cooperation between investigative bodies and the judiciary.

Recognizing the importance of the fight against high-tech crime worldwide, international organizations and authorities have undertaken and must continue to undertake activities to ensure the homogenization of judicial systems and investigative actions in all countries. This harmonization is achieved through resolutions, conventions, recommendations, guidelines, thematic conferences, standards, international workshops and the like. In particular, it must be coordinated by international organizations such as the International Telecommunications Union (ITU), INTERPOL, the United Nations Office on Drugs and Crime (UNODC), the G8 Group of States, the Council of Europe, the Organization of American States (OAS), the Asia Pacific Economic Cooperation (APEC), the Organization for Economic Cooperation and Development (OECD), the Commonwealth, the European Union and international standardization organizations [Schjolberg, 2008].

It can be said that ITU is the most active UN institution in the field of global legislation on high-tech security and high-tech crime. The ITU is committed to the development of a global agreement / protocol on high-tech security and high-tech crime, which is extremely important for a global society.

Following the EU Guidelines, the Republic of Serbia passed the Law on Organization and Jurisdiction of State Authorities for Combating High-Tech Crime ("Official Gazette of the Republic of Serbia", No. 61/2005 and 104/2009). This law created legal preconditions for establishing an institutional framework to combat this type of crime. The "Budapest Convention" (Convention on Cybercrime) served as the starting point. In drafting all regulations relating to high-tech crime, the Republic of Serbia uses international regulations and standards in this field.

So far, among other things, the following laws regulating the field of high-tech crime have been adopted:

1. Criminal Code of the Republic of Serbia (corrected and amended).
2. Law on Information Security
3. Law on Amendments to the Law on Electronic Communications
4. Law on Amendments to the Law on Copyright and Related Rights
5. Data Secrecy Act
6. Law on Personal Data Protection
7. Law on Electronic Signature
8. Law on Electronic Commerce
9. Electronic Document Act

Three strategic documents have also been adopted:

1. Strategy for the development of the information society in the Republic of Serbia until 2020
2. Strategy for the development of information security in the Republic of Serbia for the period 2017-2020
3. Strategy for the development of the information technology industry for the period 2017-2020
4. Strategy for the development of electronic administration in the Republic of Serbia for the period 2015-2018. together with the Action Plan for its implementation for the period from 2015 to 2016.

In order to ensure the proper functioning of the corporation, it is necessary to continuously undertake a number of preventive tactical and technical measures and actions in order to prevent any threats. If this is to be achieved in the corporation, then it is necessary for the management in charge to be adequately trained and educated to provide the basic function of the corporation. This includes, among other things, a good knowledge of criminal measures and actions by all those who are tasked with security. [Skakavac & Skakavac, 2010]

For the functioning of a company or corporation, it is necessary for the management in charge of security matters to organize and function properly. If this subject of safety is not adequately trained and educated for work performed within its jurisdiction, risks in the functioning of the parts or the corporation as a whole may be possible, and the consequences may be serious.

The security management systematically organizes and implements physical and technical security measures, as follows [Skakavac & Skakavac, 2010]:

1. the security of all persons during their stay in the company, and in particular the management of the company;

2. securing all facilities and premises of the company;

3. security of all types of meetings organized in the premises, in particular those where certain significant persons attend from the company's management or from outside;

4. security of special transport in the organization and for the needs of the company;

5. securing and protecting information systems, data and documentation.

In order to carry out tasks within its competence, and in order to ensure the functioning of a particular company, the security management must apply a number of anti-crime actions and measures. It is understood that this personnel must be exceptionally trained and qualified for the application of certain measures and actions. This means that these personnel have completed the relevant security and criminal faculties, but not only that. We also mean continuous education and specialization of security managers in performing these extremely responsible tasks, as well as modern technical equipment.

Managing incident situations involves controlling and detecting security-related events in the functioning of the KIS, as well as responding adequately to these events. The main task is to detect possible adverse effects and their analysis, as well as to plan and develop activities to prevent and eliminate possible harmful consequences. It is necessary that a specialized team deals with this safety business.

This security segment is becoming more and more important both for individuals and for the society as a whole (more and more jobs are done using IT). Organizations (public and private sector, associations and corporations) need to understand and accept their responsibility towards the public good, their membership, and other stakeholders. This responsibility includes the obligation to have a program in the case of "extraordinary criminal acts", which defines and implements the process for its own well-being and security.

MANAGEMENT OF CORPORATE SECURITY

The term “security management” in the broad sense, means deciding on the security objectives of the organizational system, the ways and means to avoid adverse impacts that come from the environment or the organizational system itself, or that their harmful influence is diminished. Security management, therefore, signifies the management of resources aimed at achieving the set security objectives. According to theoretical concepts, security management implies the design, organization and management of the security system in a way that removes the conditions for the emergence of a phenomenon of security threats, such as terrorism, sabotage, business and industrial espionage, accidents at work, Security management can be conditionally divided into: management in security organizations; security management in state administration bodies, public services and activities; and security management in income (business) organizations [Skakavac & Milanović, 2011].

Today, no modern company can be imagined in which top management does not attach great importance to security management at all levels of making important business decisions. Namely, the management function is not only related to the physical and technical protection of the corporation, as the security management has traditionally been treated in the past. In addition to classical security features (assessment, planning, organization, management, control), security management today collects, processes and delivers many important data to top management. They can refer to the employment process, the competitive company, the situation within the organization itself and outside, partner organizations, etc.

One of the most important functions of security management is the collection of qualiate operational data and information relating to possible risks or forms of neglect, both for the corporations themselves and their employees. The collected data and information of a security character are the basis for performing a quality security assessment based on it and making good plans for taking measures and actions in order to prevent unwanted consequences for the corporation, its assets, interests and employees. The data and information that indicate the criminal forms of endangering certainly deserve special attention, whether endangering is external or internal. Adequate quality management, thanks to good organization, division of tasks, assessment and planning, timely information on possible forms of threats, timely assessment of the security situation, planning the necessary measures and actions to prevent and interrupt certain criminal activities and, in cooperation with the competent state authorities, take measures on detection, detection and deprivation of the freedom of offenders. The management of each corporation is very interested in having a well-selected, personally-filled and well-chosen security management. It is particularly interested in having the Chief Security Officer who will execute his security task extremely responsibly and professionally. Its role is certainly the most important for the safe functioning of each corporation. From his engagement, evaluation and planning, the overall safety of the corporation depends to a large extent. His function is permanent, it is expressed in continuity, and is especially important in certain extraordinary events and events in which the corporation or some of its parts may find themselves.

That is why, for each corporation, a profile of the security manager, that is, the first security officer in the corporation, is important. The previous professional literature has pointed out and outsourced the essential characteristics that a modern security manager should have. In addition, the experiences of corporations, especially large companies, both domestic and foreign, are very important, which through the privatization process have bought certain important economic entities in this region [Skakavac & Milanović, 2011].

Staffing is one of the key issues in the security plan. On the one hand, man is the bearer of security, and on the other hand he is the most vulnerable element and the greatest potential danger. Especially since the increasing dependence on staff, possessing a range of skills, preferences, various knowledge and motivations, until recently unknown, results in a host of previously unknown corporate security issues. The confirmation of this conclusion is also the fact that these personnel are entrusted with high value assets and all data used in the corporate information system (CIS). The value of investments in equipment and software, the value of collected and regulated data, and especially the functional value of CIS, are an important factor for special attention to human resources, in every sense.

In CIS that require a higher level of corporate security, or in which the security component is present, in the selection of these personnel the criteria should be much wider and stricter. For adequate personnel, together with expertise, it is necessary that they constitute a complete personality, moral, physically healthy and psychologically stable. In addition to biography and performance without “stains”, a doctor’s certificate of adequate health condition is required. It is appropriate to use interviewing techniques and surveys to gain knowledge of attitudes, feelings, plans and desires, as well as appropriate types of testing of knowledge.

Protection is the people, and their awareness and competence are the basic measure of safety. Therefore, in order to successfully accomplish this task, the maxim of “the right man to the right place” is very important, which in this case should mean that tested, reliable and, very importantly, qualified people occupy key positions. [Petrović, 2007].

The challenges faced by the company when considering capacity in terms of providing cyber security and in line with the existing and necessary personnel are the following [Sutton, 2017]:

- The organization must define a cyber security requirement because it has data, information and strategic direction. The IT sector must use good security practice to turn this requirement into technical guidelines. The human resources sector, in consultation with IT staff and business function, must provide adequate staff training to support this requirement.
- If an organization can allocate resources for internal IT jobs, it is often assumed that these staff members also need to take responsibility for cyber security. This is a big mistake because it can conflict with one of the main principles of cyber security - the segregation of duties.
- In cases of IT outsourcing, there is a tendency to overlook or undermine the need for good cyber security when concluding a contract, since those who negotiate may not have enough knowledge or can be ignored considering it unnecessary cost.
- When a security function is transferred to outsourcing, it is often perceived as a transfer of responsibility, not a delegation. The principle that must be applied is that organizations can delegate implementation and information security obligations but must be responsible for ownership.

- The emergence of additional financial burdens for an organization that develops and implements a cyber security framework is a common case, and obtaining a capital or operational budget approval can be a challenge.
- The effectiveness of the cyber security strategy depends to a certain degree on an organization that needs to have a clear picture of risk management for information security, which sometimes is not the case.

From all of the above, it is clear that one of the elements of staff care is their education, especially given the fact that knowledge is the main driving force of society and the main precondition for progress. Knowledge is the capital of the corporation, as well as its employees, who are able to acquire theoretical and practical knowledge as an element of satisfaction with the business they deal with, and thus increase the security of the corporation. A set of related knowledge, skills, attitudes and abilities enables staff to effectively perform certain work activities.

The EU Cyber Security Strategy provides for national education and training programs in the area of network and information security, such as: network security and information training in schools, network and information security training and security software development, and the protection of personal data for students of information technologies and computer science and basic training for employees in the state administration.

ENISA (*European Union Agency for Network and Information Security*) recommendations for national cyber security strategies include the development of national programs for information security training, as well as independent courses at universities that would not only deal with the technical aspects of cyber security, but would offer a more comprehensive approach to this area. In order to develop education programs, ENISA proposes the creation of a catalog that maps the labor market in the field of information security and formulates programs in accordance with the observed shortcomings of the available professional staff.

Developing technical and political capacity of institutions and organizations is also one of the priorities of almost all international forums, as well as the European Union itself. Due to the complexity of the area itself and the fact that no one can alone defend himself from cyber attacks, capacity building requires a multidisciplinary approach and cooperation between the public, private and civil sectors. This can be done by investing in specific capacity building programs in Serbia, as well as through systematic use of existing global programs of international bodies and organizations such as the Council of Europe, ENISA and ITU, forums such as the Internet Governance Forum or the Global a forum on cyber expertise, companies such as Microsoft, professional communities such as the FIRST community of CERT and independent and educational institutions such as the Diplo Foundation, the Geneva Center for Security Policy (GCSP) and DCAFa. Capacity development, especially long-term education programs, are one of the basic elements listed in the guidelines for writing national cyber security strategies of various international bodies and organizations. In addition to providing a platform for more efficient and comprehensive national cyber security mechanisms, investing in future generations of experts contributes to the position that a country can strive to take in the field of cyber security in the future. Strategic investment in building capacity and capabilities in cyber security positively influences the transformation of the labor market, which should respond to the creation of families of new jobs in the coming decades, and in particular to the growing demand for skilled labor in this area in relation to the labor market offer. Although the development of educational programs dealing with cyber security issues both at technical and at the political level requires significant investments and resources, at the same time there are numerous programs and funds that make such aspirations more accessible [Kaurin & Anucojić & Skakavac, 2017].

Today distance education or e-learning is very. The characteristics of this type of education are: lower price, no special premises needed, can be used from any place at any time, the pace of training can be adapted to the user, can be individual or group, can be combined with other forms of education, there can be online updating of the content (innovation), it is not limited by the number and place of residence of the users, and more. E-education provides a platform for a well-designed, learner-oriented, interactive, accessible, efficient, easily accessible, flexible and significantly distributed and facilitated environment for education. Particular attention is paid to the safety and reliability of these systems. The basic requirement is the existence of an appropriate IT infrastructure [Najwa Hayaati Mohd Alwi, Ip-Shing Fan, 2010]. Within the corporation, an e-learning system for your own needs and needs of business partners can be organized. This is significant for large corporations with a large number of branches in different locations and / or countries and corporations of particular security interest.

CONCLUSION

Cyber security, first of all, should be considered from a personal point of view. It is important to know how personal information is stored and whether it is used appropriately. It is necessary to proactively protect the data and this begins with the responsible behavior of each subject, but at the basic level, for example, taking care of the information that is available, because each of them can be misused at some point in a certain way. For corporations, this is one of the most important business priorities. Accordingly, radical measures and activities in the organization and functioning of the information security service are unfocused. From a business perspective, it is possible to distinguish four key reasons that indicate that cyber incidents should be taken into account, and have a plan to defend individuals and organizations from cyber attacks and be prepared for an adequate response if they occur. This includes: [Sutton, 2017]:

- Applying good risk management practice that necessarily includes the risk of cyber attacks, whether planned or incidental, and whether it is directed at an individual or a company. We should be aware that the leakage of company data can begin by targeting individuals so they must apply equal priorities in such cases.
- The company has a duty towards users and they have the right to expect that the company will behave responsibly according to the data at their disposal. With this in mind soon (May 2018), the General Data Protection Regulation (GDPR) will enter into force a new legal framework that prescribes how to use EU citizen data. It obligates any organization that in any way processes EU citizens' data to comply with new rules on the protection of personal data, even if it is headquartered outside the territory of the EU.
- In highly organized sectors, organizations can comply with national or EU law; international standards such as the ISO / International Electrotechnical Commission (IEC) 27001 and sectoral standards, such as the Payment Card Industry Data Security Standard (PCIDSS) and others.

- Organizations should demonstrate good security practice as a means to achieve a competitive advantage. Larger organizations can use ISO / IEC 27001 certification until they can be identified for some acceptable schemes such as, for example, Cyber Essentials promoted by the Government of Great Britain.

Security in the cyber environment is a very complex, professional and responsible task that requires exceptional expertise and dedication of practically all participants in its performance. It is a mistake to regard it as the responsibility of the IT sector alone or solely as a management responsibility. Treatment of cybersecurity as a business risk is not effective if individuals will already be effective exclusively since it is global. Developing a secure environment implies the application of appropriate standards and methodologies that facilitate and serve as a roadmap in carrying out these tasks. In this way, in addition to the high degree of security that the work will be done in an adequate manner, it also ensures the cooperation and the necessary level of security in the mutual communication between different participants in the application of IT. Equipment and software vendors also play a role in the security system, enabling their clients to implement a security system in accordance with their needs, using various options. Companies that provide services in the application of IT play a significant role, ranging from designing projects and their introduction to the function of renting complete information systems, guaranteeing an adequate level of functionality and security.

By introducing of the security system into the function, only the beginning is achieved. It is necessary to continually improve it, not only because of removing the observed shortcomings and the application of new technologies and functional capabilities, but also because of the continuous struggle with high-tech crime, which also advances, monitors technological development and takes on new modes of operation. One should not forget that security in the cyber environment is actually a subjective feeling that is not based on a mathematical calculation and probability, but a psychological reaction to known risks and security measures. The cyber environment itself does not pose a danger, it is dangerous because of users who can endanger themselves and others. In this respect, the essence is to understand the concept of risk and security, as well as the developed security culture. The first step on this path should be to raise awareness of cyber crime and cyber security. Continuous work on developing awareness and improving digital competencies relies on the continuous education of all subjects. The terms related to this topic are digital literacy or digital competence and relate to the ability to use technology at work, at leisure and in communication [European Commission, 2015], which means that in addition to technical knowledge and skills they also include critical and creative use of information, solving problems in the digital environment, as well as the socio-ethical aspects that also include the safe use of digital technology [Kuzmanović, et al 2016].

REFERENCE

Anucojić D.,(2010), *Zaštita informacionih sistema u korporativnoj bezbednosti*, Zbornik radova, Naučni skup „Dani bezbjednosti“: „Korporativna bezbednost – rizici, prijetnje i mjere zaštite“, Banja Luka, 2010. godine;

European Commission, (2015), Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. A Digital Single Market Strategy for Europe, http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52015DC0192

Kaurin T., Anucojić D., (2011). *Zaštita informacionih Sistema i podataka*, Fakultet za pravne i poslovne studije dr. Lazar Vrkatić, Novi Sad.

Kaurin T., Anucojić D., Skakavac Z., (2017), *Difuzija moći u Sajberprostoru: izazov ili pretnja bezbednosti*, Savremeni izazovi međunarodne bezbednosti, monografija od međunarodnog značaja str. 203-233,

Kaurin T., Skakavac Z. (2016), *The importance of digital forensics of mobile devices in detecting and proving criminal acts of organized crime*, 5th International Scientific And Professional Conference The Police College research days in Zagreb, New Technologies and Methods Used for Improvement of the Role of the Police in Security Matters, University Press,Vol. 9 No. 5.

Kaurin T., Skakavac Z., (2017), *Safety Culture Of The Young,* International Monograph of Scientific Research Intedisciplinary Projekt, Publisher: Faculty of Business Studies and Law; Faculty of Strategic and Operational Management; Austrian Institute for European and Security Policy/AIES Wien, Austrija; Institut za korporativne varnosne študije, Ljubljana, Slovenia, 2017., poglavlje: Safety Culture of the Young People in Cyberspace, str. 127-142,

Kuzmanović D., Lajović B., Grujić S., Medenica G., (2016), *Digitalno nasilje – prevencija i reagovanje*, Ministarstvo prosvete, nauke i tehnološkog razvoja Republike Srbije i Pedagoško društvo Srbije, Beograd http://www.digitalno.pedagog.rs/

Najwa Hayaati Mohd Alwi, Ip-Shing Fan, (2010), *E-Learning and Information Security Management*, International Journal of Digital Society (IJDS), Volume 1, Issue 2, June 2010, http://infonomics-society.org/wp-content/uploads/ijds/published-papers/volume-1-2010/E-Learning-and-Information-Security-Management.pdf

Pleskonjić D. et al, (2007), *Sigurnost računarskih sitema i mreža*, Mikroknjiga, Beograd.

Schjolberg S., (2008), *The History of Global Harmonization on Cybercrime Legislation - The Road to Geneva*, http://www.cybercrimelaw.net/documents/cybercrime_history.pdf

Skakavac Z., Malinović D., (2011), *Uloga menadžmenta bezbednosti u zaštiti korporacije od kriminaliteta*, Zbornik radova, V naučni skup: „Dani bezbjednosti": „Razvoj sistema bezbjednosti i zaštite korporacija", fakultet za bezbjednost i zaštitu, Banja Luka, 2011. godine;

Skakavac Z., Skakavac T., (2010), *Kriminalističke mere i radnje u korporativnoj bezbednosti*, Zbornik radova, Naučni skup „Dani bezbjednosti": „Korporativna bezbednost – rizici, prijetnje i mjere zaštite", Banja Luka, 2010. godine;

Skopik F., (2017), *Collaborative Cyber Threat Intelligence Detecting and Responding to Advanced Cyber Attacks at the National Level*, FL:CRC Press, Boca Raton.

Solms R., Niekerk J., (2013), *From information security to cyber security*, Computers & Security, http://dx.doi.org/10.1016/j.cose.2013.04.004.

Sutton D., (2017), *Cyber Security: A practitioner's guide,* BCS

Symantec. Internet security threat report, Volume 22. https://www.symantec.com/en/ca/security-center/threat-report; 2017 von Solms R, van Niekerk J, (2013), From information security to cyber security, Computers & Security http://dx.doi.org/10.1016/j.cose.2013.04.004.

UDC 351.86

PLACE AND ROLE OF CORPORATE SECURITY IN THE NATIONAL SAFETY SYSTEM

Boriša Lečić
Faculty of Law and Business Studies dr Lazar Vrkatić, Novi Sad

One of the primary goals and demands of the modern world is to achieve the highest level of security in all spheres of social life. Today security is not only a strategic goal but also an essential global problem, since some of the perilous factors today have assumed quite new shapes and dimensions, targeting directly the national economy and the economic system. Implicitly, a securityally unstable economy induces a potential social danger for the system of national security. Under such conditions, modern security, as a phenomenon, from a doctrinal point of view must be perceived in a wider context. Strategically, it strives for the concept of universal security that integrates various components - geopolitical, economic, social, information, ecological, energy, etc. Modernity shows that the successful development of the most developed national economies in the world today is based on the security of the economic, social and ecological system, together with many contemporary contradictions and inequalities, such as security challenges and risks that are increasingly endangering global security. As a result of numerous social changes and processes, corporate security has emerged that needs to ensure the protection of businesses and entrepreneurship in a preventive, long-term and continuing manner. Consequently, it directly and indirectly, organisationally and functionally can play an important role in achieving the highest level of national security that will be discussed in the topic of this paper.

INTRODUCTION

Intensive social changes, especially the processes of political and economic globalization, accelerated technical and technological development, the integration of multinational companies, their financial and investment power, hegemonic polarization, have strongly influenced the understanding of the general notion of security, especially its content. In the constellation of new economic ideologies, transnational economic development with all its contradictions and inequalities necessarily demands that security, as an international category, unreservedly, continuously and at all costs, follows these social changes and processes in order to ensure unhindered, dynamic economic development.

In parallel with the development function, globalization processes, along with the existing ones, have generated a number of new, destructive threats and risks for international peace and security, creating a fertile ground for economic destabilization. This has led to the fact that, over time, the traditional functional concept of the state is increasingly overtaken and replaced with new forms of transnational and regional associations, motivated exclusively by interest-based profit reasons, gradually taking over individual state powers, among others, security.

In such circumstances, a strong shift has also emered in terms of an innovative understanding of the concept of security and its function.

In the new geopolitical configuration, security is increasingly gaining a corporate dimension too, putting economic issues at the center of interest. In such social conditions, especially in the context of a new spectrum of security challenges, threats and risks, the military component of security is increasingly being pushed into the other, more precisely, "the phase of latent risk threats is coming to an end, invisible dangers become visible, and modern society becomes a risky society" [Ulrih, 2001].

In the theory of international security, it is openly questioned whether there is a crisis in the management of the national security system because practice shows that the dominant position, gradually but increasingly, is occupied by "non-state factors of transnational security structures" [Despotović, 2017]. The new global management order shows that in a large number of European countries there is a growing presence of private security in the public sector, that is, "public services are increasingly secured by private entities, especially what is called security and equality" [Atali, 2010]. This in itself can be termed a paradox because in this way the system of national security, conditionally speaking, is ignored and put aside.

In complex operating conditions of the modern, globally transformed world, corporate security as a function increasingly becomes important in the face of a number of everyday challenges, tasks and problems that security management has to deal with without delay and respond to them with modern organizational and management methods. The role and significance of corporate security is particularly evident in countries in transition, such as Republic of Serbia, where privatization processes are still ongoing, and the systemic, conceptual transformation of the national economy is strongly present. In transition "societies, the impact on the prevention of security incidents has been reduced, as well as on the overall organization and ability of crisis management and the elimination of its consequences" [Trivan, 2012].

The key issue are the potential, but quite realistic risks and challenges that large global companies can make on national economic systems, producing indirect effects and effects on the national security system. This correlation is complex and specific because it is based on a conflict of opposing interests, where multinational companies, without selecting funds, are primarily seeking to achieve enormous profits, and the state is striving for a stable, general economic interest and intensive development. Economically influential economic entities do not have any prejudice in their business functioning. They are managed exclusively by their partial interests, which include the possibility of a very real, interesting influence on the national, political and economic establishment, where for example through the control of cash flows, they can indirectly produce a danger to the national interests and the national security system.

It is evident that the new social and business environment with new challenges, risks and threats has modeled the modern concept of corporate security. Previous traditional, typical security mechanisms have shown that companies are very poorly managing risks, especially in evaluating early business and security risk indicators.

Due to the lack of a general, effective model that would continuously manage the crisis, contemporary practice inevitably requires the development of a state and private security partnership in which corporate security, as a strategic multi-dimensional function of the company, should have the status of an inevitable component of the national security system.

CORPORATE SECURITY - ROLE, IMPORTANCE, PERSPECTIVE

The strategic goal of each business is to achieve as much profit as possible, ie continuous business success. In order to achieve this, responsible corporate governance involves first preventive identification of potential risk factors, their ongoing, proactive analysis, and on the basis of that the adoption of appropriate safeguards and activities, including security. The ultimate goal is to completely eliminate or minimize the effects of endangering factors through systemic control mechanisms. An indispensable condition for this is that corporate security is an integral part of each company's strategic business documents and is at the top of its priorities rather than being traditionally treated as an expense.

The primary mission of corporate security is to create an environment in which businesses can survive on the market in the long run in order to ensure a stable business continuity. Its role is reflected in the ability to quickly anticipate the threatening internal and external risk factors (market, state of the economy, regional movements, investments, administrative procedures, etc.) in order to take adequate protection activities. A corporate analysis of potentially possible etiological risk factors allows them to quickly respond to business and remedy them in the shortest possible time.

Edward Friman, professor of business administration at Darden University of Virginia, spoke about the strong effect of internal and external factors on the business activity of a company. Taking into account the corporate strategy and stakeholder theory, in the 1980s, he set the principle of "stakeholder", according to which every business entity faces the effects of external and internal factors, which are interactively interconnected, affecting one another. According to Friman, they include government and management, professional and civil authorities, employees and consumers, importers and creditors, among which there is a constant rivalry. According to him, between these parties, it is very important to develop a cooperative relationships in order to ensure a high level of corporate security [Freeman, 1984]. He believes that by mutual consenting communication and business dialogue of rival parties, they avoid security risks and establish the necessary relationship of trust, which is one of several functions of corporate security.

For "government, the company is at the same time a source of state power and public policy interference" [Barnet & Muller, 1974], which makes it important to establish a compromise balance, abstracted by security risk. In contemporary conditions, corporative security must at the same time optimize two diametrically opposed goals - on the one hand, to enable a stable, growing, business-evolving trend, and on the other hand to prevent ever more sophisticated attacks on corporations [Murray & McKim, 2000].

The business future of the company should be in their hands, which depends to a large extent and is realized through the function of corporate security that enables business in the most complex, extraordinary circumstances - crises, catastrophes, etc. The beneficial effects and the capital contribution of corporate security are reflected in the fact that it significantly participates in the realized total profit of the company, thereby materializing and valorizing its concrete engagement through the output profit. However, its results are often not in practice tangible and visible, and can hardly be mathematically precisely quantified, which, among other things, is a common feature of the engagement and operation of other security entities.

Although corporate security is defined as a state or absence of business risk, it can not be regarded as a static category, but rather as a dynamic, developmental and continuous activity where the permanent security measures successfully overcome the negative effects of business challenges and risks. Therefore, it is "planned, organized and based on the law, an independent or joint activity and function of organizations, private and / or professional agencies, dedicated to their own protection or protection of others, as well as the protection of appropriate persons, premises, facilities, businesses or activities that are not covered by the exclusive protection of state authorities "[Stajić, 2008]. Its significance and role is effected not only on the enterprise, company, business system, but also on the individual, society as a whole, directly or indirectly influencing and giving appropriate contribution to the national security system.

COMPLEMENTARITY OF NATIONAL AND CORPORATE SECURITY

The interaction and interdependence of the modern state, the modern economy and the system of national security have become essential legislation today. National security viewed from the point of view of its primary goals - survival of the state, nation, population, political autonomy and independence, territorial integrity, social standard [Baylis & Smith, 2005] - is of special significance and inextricably linked to the economic strength of the national economic system. A stable economic system is a strong base and a guarantee of national security. On the basis of this connection, a relatively new concept of corporate and economic security has been developed, which by its protection mechanisms protects not only its own business interests, but also in parallel, contribute to the integrated functions of national security.

In some European countries, most of all in Great Britain, from the 18th century, they hold the view that "national security is inextricably linked to economic well-being, and particularly to trade" [Moller, 2003].

It is evident that security challenges and risks, such as contemporary forms of international terrorism, organized crime, economic and financial crises, money laundering, corruption, etc., are present in the modern epoch of social development in all spheres of social life, causing negative and destructive effects in the field of politics, economics, energy, ecology. This inevitably requires a continuous and proactive role and symbiosis of the joint action of a large number of state and non-state actors in order to achieve the required level of national security. Of course, this implies systemic cooperation based on institutional foundations, and not simple, individual and isolated activities of security actors, which is confirmed by today's practice. The national security system must function in an integrated manner, interacting with others, not only state, but also social and private security entities that include corporate security. Systemic harmonization is needed as well as a unique, functionally connected way of reacting to the listed global threatening factors, since they are inevitably required by current dynamic processes. The complementarity of the functions of national and corporate security is reflected in the fact that both of them, due to preventive reasons, must perceive in a timely manner and precisely identified security risks and threats, otherwise their position and role would be without justification.

Institutional-systemic connection is very important and necessary because the achievement of universal security is a strategic doctrinal definition of the political system of each state, This can not be achieved without the integrated functioning of the national security system (state and non-state), which is a subsystem of the political system. The complementarity and functional connection of parts of the system should be based precisely on the continuous and directional exchange of security-relevant information. As an example of the disharmonious functioning of the national security system we can mention France where seven intelligence security services were completely unrelated, which was reflected in the failure of the anti-terrorist activity. This later resulted in the centralization and integration of all parts of the national security system in order to achieve national security interests [Lečić, 2015]. Without this, it would be a mechanical, dysfunctional, unconnected set of state and non-state security entities where the latter would, in fact, be marginalized regarding security.

The need for the establishment and development of institutional cooperation between the public and private security sectors was also pointed out by the European Commission, which in 2009 issued an official document called the "Announcement", which gave concrete recommendations to EU member states, emphasizing the importance of this issue [European Commission, 2009]. Guided by this document and the National Security Strategy, the Republic of Serbia also points to the need to include a wide range of state and non-state actors in the national security system, especially from the sphere of private security, economy, energy, information technology, ecology,

The actualization of the concept of "human security", based on a new system of values that, in addition to the survival of the state, puts economy, well-being, social security and development at the forefront, insists on inclusion in the system of national security of other factors too - private and non-state. In such a constellation of security subjects, it is unclear whether corporate security is an indispensable component of national security, because economic resources of a country, as a source of political and military power and influence, are at the very top of strategic security priorities. In practice, separate functioning of public, private, and consequently, corporate and economic security is practically impossible, since the modern forms of security risks and threats necessarily make them mutually dependent.

An important prerequisite for a public and private security partnership required by a higher, general interest, is the appropriate normative legal framework that would be the first step towards systemic incorporation of corporate security into the national security system. A particular aspect of legal regulation would be the issue of coordination between the parts of the system understood as "the process of integrated activities for the effective achievement of goals" [Mooney, 1947]. This is of paramount importance because modern economic trends through the political process of globalization increasingly relativize the classical security functions of the state apparatus, especially in the economic sphere. More precisely, the national security system in the broader sense basically guarantees only an elementary level of security, while the objectives of corporate security on the other hand are much more complex and multi-dimensional. It is believed that "the new situation, in some cases, caught security services unprepared and that as such they experienced numerous surprises and made mistakes because their organization, methods and means of work were directed to different opponents, and the enemy appeared in a completely new form that required radical changes; this process is in progress "[Stajić, 2008]. Corporate security must fully and in the long run provide a stable business environment and conditions for protecting the vital business and property interests of the company from internal and external threatening factors.

For these reasons, it is inevitably insisted that the security management of international companies that operate on our national market at all costs must analyze and continuously monitor the dynamics of the global functioning of the environment, with the aim of controlled management and monitoring of the effects of associated risk factors [Kytle & Ruggie, 2005].

COMMON CHARACTERISTICS OF CORPORATE AND NATIONAL SECURITY

Connection relations between corporate and national security are based precisely on the "inseparable ties between the economy and the state and their mutual interests" [Anđelković, 2015], namely, the "close connection of security as an attribute of the state with its economy, because just like economy is a necessary factor of security, in the same way safety is a prerequisite for a stable economy " [Savić, 2008].

As an integral component of the state apparatus, the state security system is authorized to apply force on its behalf and for its account, in accordance with positive legal regulations [Edmunds, 2007] as the ultima ratio for the protection of vital national interests

The new security movements conditioned the dislocation of the notion of security from the previous "predominantly military sphere in completely new areas - economy, energy, ecology, social security, including security of the individual and society as a whole" [National Security Strategy of the Republic of Serbia, 2009]. In order to accurately and timely identify unpredictable, transnational and asymmetric security risks and threats, intragational processes in the security sphere are becoming more intense which at the national and broader level requires involvement and engagement of all entities that contribute to the achievement of a higher level of national security. The system thus established requires that there must be a mutual cooperative relationship between all of its constituent parts, and therefore it rightly raises the question of whether corporate security is compatible with the national legal security system at the national level [Huntigton, 1993].

The need for organizational and functional cooperation between corporate and national security is referred to by several common features and interests that require their coordinated and communicative action.

First, their common, primary goal is the protection of vital interests, on the one hand, of the state, society and citizens, and, on the other hand, economic interests, resources and capacities of companies. Under the conditions of contemporary globalization, political-economic processes the perilous factors have significantly evolved, taking quite new forms and dimensions in relation to the period of the "cold war". This has led to an equivalent coincidence and interweaving of national interests and interests of multinational companies in whose protection they use identical mechanisms through corporate security.

Second, guided by the fact that the crisis situation in the economy is always a fertile soil for economic crime, it is logical that one of the basic functions of the system of national and corporate security is opposing all forms of organized and classical crime. Combating corporate crime (business fraud, theft, bribe, corruption, economic espionage, sabotage, ecological accidents, etc.) are the key tasks of security management. Although these tasks in the security practice of national and corporate security are achieved through different methodological approaches and mechanisms, the ultimate goal and the result of corporate and national security, observed through a function or state, in this area is the reduction of the crime rate.

In this regard, it is important to recall that the practice of corporate security shows that there are experienced and trained personnel among its members, with basic and highly specialized knowledge and skills in combating certain forms of crime that in the detection and proving of criminal offenses can form a partnership between public security organs. In this regard, the fact is that in the private security sector management, especially in foreign companies, with a significant number of former members of the police and security structures with enviable professional capacities are engaged, and this is a valuable potential in the function of the national security system. By contrast, through backward cooperation and interaction, the subjects of national security in a narrow sense give a strong contribution to raising to a higher level of security culture and awareness of members of corporate security management. Security culture is an extremely important factor in preventive identification of potential hazards and risks because it "forms the context within which the security positions of an individual are developed and maintained and promoted by various security behaviors" [Mearns, 2003].

In this way, not only corporate economic interests are protected, but the beneficial effect is reflected in political, economic and social stability and security, as well as on the national security of the state and society as a whole.

One of the features that links corporate and national security is the power of their members that enables them to perform effectively the protection of persons, property and business, as well as state and national interests. Their application must strictly be based on the constitution and law, because otherwise their abuse leads to violations of guaranteed freedoms and rights. For example, the activity of members of corporate security is operational-research and informative-intelligence in nature, and it is focused on collecting, processing, analyzing, evaluating data and on that basis they make appropriate decisions. The same methodological approach is used by police-security structures in carrying out national security tasks.

Correlation features of corporate and national security come to the fore in terms of mutual exchange of security-relevant and other data. The corporate security management (detective activity) is obliged to notify the police and the competent public prosecutor without delay about the knowledge that an offense has been commited that should be prosecuted by law and authorized police officers must have access to the relevant records. On the other hand, representatives of corporate security may, in accordance with the procedures regulated by law, provide a written explanation of the requirement and contact the state administration bodies and other state bodies that exercise public authority and ask for appropriate data and information from them (on identity, place of residence, real estate, pension and disability insurance, etc.).

Since members of the corporate and entities of the national security system deal with the collection, processing and analysis of data, the important issue is the security aspect of their protection, that is, the unauthorized handling of confidential and classified information. The questions of categorization of data, their degree of confidentiality and standardized handling of documents are very precisely and thoroughly regulated by the laws and by-laws of the subjects of the national security system, unlike the corporate security structures where systemic deficiencies and omissions are observed. This segment of corporate security is rather underdeveloped, which in the circumstances of the concrete case can have serious and unimaginable implications for national security, especially when it comes to confidential procurement that is realized through private companies for the needs of state structures.

A special aspect of security protection of classified and business data in corporate and national security systems is computer systems and networks or the so-called “social engineering”, which according to the practical analysis in modern conditions is a frequent target of attacks by competitors.

The coherence of the goals and tasks of corporate and national security is reflected through their primary function of preventive action. It manifests itself not only in terms of precise identification and perception of potential threatening factors, but also in terms of their effective neutralization. This is accomplished through the anticipation of their certainty and the analysis and assessment of the effects of corporate and national interests. Although crisis situations can not be completely overcome, a proactive approach at a perceived level is of paramount importance. It opens the possibility of controlledly managing national or corporate security risks and threats, in contrast to the opposite situation when a crisis factor manages the system, since it is created, is “alive” and active. More precisely, it is much better to prevent the occurrence of adverse effects through prevention, and to repair harmful consequences. through reactive action, by the most effective methods.

On the other hand, security prevention is one of the basic principles of national security policy in suppressing security risks and threats that are exclusively dimensioned in the political and economic system. It is these common interests of the economy and politics that point to the inescapable need of “integrating corporate security into the national security framework” [Keković, 2004]. The effectiveness of the national security system is measured by its ability to recognize, pre-empt and fully or partially eliminate or minimize the impact of the negative effects of internal and external security risks, and it can equally be said for corporate security which, by removing economic risks of business, ensures the long-term sustainability and profitability of business entities.

One of the common elements that marks corporate and national security is the fight against terrorism as a global phenomenon, which has a very strong impact on security in general and in particular on the economy. Terrorism can not be viewed and resolved locally and in a isolated way, as it is one of the biggest challenges of modern democracy. It is necessary to have a generally accepted, universal strategy based on efficient international cooperation of all subjects of international law. In the basis of this international cooperation, which should not only be declarative, there should be institutional exchange of the information that are important for security, because no country is large enough that it does not need assistance in solving this problem, and no country is too small to contribute [Doorey, 2014]. On the other hand, it is obvious that the concrete results of a comprehensive and lasting suppression of terrorism are more modest than they should be, especially nowadays, when this phenomenon escalates increasingly, rising to the level at which terrorists have managed to form their own quasi-state [Lečić, 2017].

Although corporate security, as a business function, operates within the organizational structure of the company, its contribution to national security, in the context of expressed terrorist threats, manifests itself through the security protection of vital facilities of “critical infrastructure”, which can at any moment be a potential target of terrorist activities. This is beneficial to the specificities of the corporate environment, social tension, easy availability of weapons, the activities of rebels and other extremist armed groups that make the business activity of large companies unstable. As an example of critical infrastructure targets, we can mention large world oil companies that, as a personification of the military and political power of states, increasingly become potential terrorist targets.

In the long term, the implications of terrorism on the business activity of companies are reflected not only in human and material sacrifices, but they also strongly affect the confidence of clients and investors [Barry & Nedelescu, 2005], as well as the overall instability on the market.

The term “critical infrastructure” is derived from Western security legislation and theory, and it includes the assets that are vital to the smooth functioning of the social, political, economic and cultural systems of a state. An equivalent term used in our legislative and security theory and practice is “objects of interest for defense”, “mandatory secured facilities” and “objects of special social interest”. It is precisely “critical infrastructure” that is a good example or experimental zone where in practice the full and optimal co-operation between the public and the private security sector should be achieved. Certain European countries such as Germany, Great Britain, Belgium and Spain have developed this coopeartion in which they recognize the beneficial security effects and capacities of the private security sector. There is a specific forms of public-private partnership between security entities in these countries. They are precisely regulated and institutionalized by being incorporated into national regulations and reflected through their regular and everyday communication. In some cities of these countries, private security operators have completely interconnected themselves and got united with local police structures so that they can exchange safety-sensitive information on their observations through the control operational centers and pre-determined contact points (a permanently open telephone line). The mutual cooperation has been developed to the extent that several thematic seminars on security education is organized several times a year together with training of staff for quick response in incident situations, as wells as joint assessing and analyzing of potential security challenges and risks at local, regional and national level level, etc.

These models of public-private cooperation have proved to be very successful in practice, especially in the field of preventive neutralization of potential terrorist activities as well as other low-intensity risks, and they support the argument that the non-state security sector, both institutionally and systematically, contributes to the stability of the national security system.

Therefore, today the most common forms of threatening the business interests of multinational companies are terrorism and other forms of political violence, which is the primary focus of the intelligence and security structures of the national security system, naturally in a coordinated and planned connection with the system of company and private (corporate) security.

CONCLUSION

Observed from the perspective of national security, corporate security has a very high significance, especially in countries such as Serbia, where privatization processes have not yet been completed. Its contribution to the achievement of a higher level of national security is reflected in the realization of a part of the national interests that have economic significance. However, the analysis of the practice shows that the available corporate security capabilities are not adequately used or adequately represented in the national security system of our country. There are several reason for this, and one of the most significant ones is the absence of systemic, institutional-functional connection with the national security system. In order to achieve this, it is necessary to develop an appropriate normative legal framework that would be a legitimate basis for mobilizing operational capacity of corporate security in the interests of national security.

Without diminishing the effective and functional power of the primary players of the national security system (military police, intelligence and security structures, etc.), there are evident processes of intensive privatization of the security sector, which are conditioned by numerous social transformations and new emergent forms of security challenges and risks. This resulted in a gradual, but increasingly evident, transfer of security as exclusive jurisdiction and rights of the state to a private, co-operative economic level. Whether the actualization of corporate security, conditionally, is the result of the inefficiency of the state security apparatus or the implementation of security standards and trends of the modern world is a practical issue, but on the other hand it is evident that the gap between public and private security is disappearing.

In such circumstances, corporate security, in a doctrine and strategic way, should take an important place in the national security system. Although this relationship is complex, and a public private partnership is necessary, it needs to be precisely defined from the aspect of the division of competences. It should be systemically institutionalized with a clear legal and contractual framework and it must be strictly controlled. Practice has shown that only the integrated system can achieve the highest level of national security. The precondition is that parts of the system are interactively connected.

Given that the primary goal of corporate security is the long-term economic viability of an entity and the effective neutralization of internal and external vulnerable factors, it is necessary to invest continuously in corporate security strategy and policy, staff training, sophisticated security technologies, in order to achieve the highest security performance, implicitly and at the level of the national security system.

In practical terms, strategy serves to ensure that the overall functioning of the corporate security function is operatively and functionally harmonized, and that it adequately relates to various forms of security breaches of the company.

REFERENCES

Anđelković, S. (2015). *Korporativna bezbednost kao činilac nacionalne bezbednosti*, Doktorska disertacija, Fakultet za evropske pravno političke studije, Univerzitet Edukons, Novi Sad.

Atali, Ž. (2010). *Kriza, a posle*, Hedone, Beograd, str. 136.

Barnet, J.R. and Muller, E.R. (1974). *Global Reach: The Power of the Multinational Corporations*, Simon and Schuster, New York

Barry, R. and Nedelescu, O. (2005), The Impact of Terrorism on Financial Markets, IMF Working Paper Monetary and Financial Systems Department, http://www.imf.org/external/pubs/ft/wp/2005/wp0560.pdf

Baylis, J. and Smith, S. (2005). The globalization of World politics, Oxford University Press, Oxford, United Kindom.

Despotović, Lj. (2017). *Globalizacija i geopolitika identiteta*, Kairos, Sremski Karlovci, str.68.

Doorey, T. (2014), Tthe counterterrorism Challenges in Region off South-Eastern Europe, Maribor, 2014. https://www.korporativnabezbednost.rs/aktivnosti2014.php

Edmunds, T. (2007). *Security sector reform in transforming societies: Croatia, Serbia and Montenegro*, Manchester Univeersity Press, Manchesster. str.23.

Freeman, R. E. (1984). *Strategic Management: A Stakeholder Approach*. Pitman Publishing, London.

Huntigton, S. (1993). Whu International Primacy Matters, *International security*.

Keković, Z. (2004). Upravljanje rizicima u nedržavnom sektoru bezbednosti, *Bezbednost*, Beograd, Vol. 46, no. 4, str.560-572.

Kytle,B. and Ruggie, J.G. (2005). *Corporate social responsibility as risk management: A model of multinationals*, Corporate Social Responsibility Initiative Working Paper No 10, Harvard University, Cambridge.

Lečić, B. (2015). Francuski odgovor na izazove globalnog terorizma – istorija i savremenost, *Srpska politička misao*, Vol. 50, no. 4, Institut za političke studije, Beograd, str.317-318.

Lečić, B. (2017). Organizacija UN u borbi protiv savremenog terorizma, *Zbornik Matice srpske za društvene nauke*, br. 159/160, Mtica Srpska, Novi Sad, str. 889-899.

Mearns, K., Whitaker, S.M., Flin, R. (2003). Safety climate, Safety management practice and safety performance in offshore environments, Safety Science Vol. 41, no. 8, pp 641-680

Moller, B. (2003). Nacionalna, socijetalna i ljudska bezbednost – Opšta razmatranja sa prikazom balkanskog slučaja, *Ljudska bezbednost*, Vol. 1, no.1, Fakultet civilne odbrane, Beograd, str. 44-45.

Mooney, J. (1947). *The principles of organization reved*, Harper&Brothers, New York.

Murray T. and McKim E. (2000). *The Policy Issues in Policing and Private security*, Canadian Association of Chiefs of Police, Ottawa.

Savić, A. (2008). Privatna bezbednost u sistemu nacionalne bezbednosti, Prvi međunarodni naučni skup „Privatna bezbednost-stanje i perspektive", *Zbornik radova*, Fakultet za pravne i poslovne studije, Novi Sad, str.148

Stajić, Lj. (2008). Izazovi korporativne bezbednosti u svetlu savremenog shvatanja pojma bezbednosti, Prvi međunarodni naučni skup „Privatna bezbednost-stanje i perspektive", *Zbornik radova*, Fakultet za pravne i poslovne studije, Novi Sad. str.27-34.

Strategija nacionalne bezbednosti Republike Srbije, (2009). www.srbija.gov.rs.

Trivan, D. (2012). *Korporativna bezbednost*, Dosije stdio, Beograd, 2012.

Ulrih, B. (2001). *Rizično društvo*, Filip Višnjić, Beograd, str. 81.

European Commission. (2009) 615 Saopštenje Komisije Evropskom parlamentu, Evropskoj ekonomskoj zajednici i Socijalnom komitetu i Komitetu regiona od 19. novembra 2009. godine o mobilisanju privatnih i javnih investicija za obnovu i dugoroćne strukturnu promenu: razvoj partnerstva između javnog i privatnog sektora: http://ec.europa.eu/archives/growthandjobs_2009/pdf/european-economic-recovery-plan/ppp_en.pdf

UDC 316.772.4:004.738.5
343.533::004

POLITICAL ASPECTS OF CYBERSECURITY

Professor of political philosophy Boris Manov, PhD
South-West University "Neofit Rilsky", Blagoevgrad, Bulgaria

The paper asserts that the problem of cybersecurity is one of the most important problems of the contemporary world. Cybersecurity is defined as the ability of a society to prevent and reject the threats in cyberspace. On this basis, the main aspects, the nature, and the mechanisms of political cybersecurity in the communication society are identified. The conclusion demonstrates that the main main challenge before our contemporary society is to determine where the 'limit' lies not only between freedom and cybersecurity but between freedom and national security as a whole.

INTRODUCTION

The present paper will outline several key aspects of the problem of cybersecurity, its nature, manifestations and the mechanisms through which cybersecurity may be achieved, by:

A) identifying the most important characteristics of the communication society, which lead to its becoming a 'risk society', and determining the need for certain changes to be introduced of the governance and the security policies;

B) identifying the main threats to the security of cyberspace and some of the possible policies and actions through which they may be overcome;

C) clarifying the issue of the 'limit' between freedom and security as a central existential and political problem not only of cybersecurity but of national security as a whole.

THE COMMUNICATION SOCIETY

A profound and comprehensive transformation is taking place in human society in the 21st century, turning it into a 'risk' [Bek, Бек, 2001] and 'communication' [Velkova i dr., Велкова и др., 2012] society, demanding and imposing the need to reevaluate its essence and the ways through which its existence in the future may be guaranteed. In the light of their importance for security, the following main features of the communication society can be identified.

Firstly, the communication society is a society based on digital technologies and computers in the production, storage and dissemination of information, as well as the use of the Internet as a global information exchange network. In less than twenty years, the 'net' has become the most influential 'subject' of modernity. The number of Internet users at the beginning of 2017 exceeded 3.1 billion worldwide, which is a two times as much users as there were in 2008.

Secondly, new web-based services and platforms such as MySpace (2003), Facebook (2004), YouTube (2005), Twitter (2006) have been established that have qualitatively changed the nature and scope of the Network and have lead to the development of an interactive communication space. This trend is exacerbated by the 'semantically' based Web 3.0 technology built through the merger of the Internet with mobile communications and mainly with smartphones (at the end of 2016 smartphone owners are almost 2.7 billion people), which leads to a situation in which everyone - manifestly or anonymously, at any time and from anywhere, may create, distribute and consume information in the form (text, sound or image) and with the content and purpose which they deem necessary.

Thirdly, in the communication society, interconnection, even a 'merging' of the virtual and the real is taking place which in turn leads to the overcoming of the spatial and temporal limitation of the real social space.

Thus, even the boundaries between states, albeit formally preserved, are increasingly being abolished; they are becoming more 'permeable', as cyberspace encompasses all inhabitants of the planet with Internet access.

The coexistence of virtual and real space also manifests itself in the formation of a new type of in modern society - a 'virtual-real' activism. Its main characteristic is that it moves the 'center' of mobilizing citizens for participation in social activities away from the 'real' society and the various 'real' existing institutions and organizations - such as states, political parties, NGO's – to virtual 'social' networks and other 'power' centers of cyberspace. In this way, the subjects and the nature of social processes are changed, as well as the mechanisms of governing the political and social life as a whole, both internally and externally (internationally).

Fourthly, the communication society is a 'risk' society. The 'risk' of the ever-growing 'virtual-real' world is generally manifested in:

A) In the technical and technological aspect, the threats related to:

- the various types of 'software' infections on computers and computer systems (150 000 malicious codes 'infect' over 1 million people worldwide every day) [News. bg, 22.10.2012];
- the alarming amounts of spam messages on the web (more than 1/3 of the daily internet exchange is characterized as 'spam') [Ibid];
- the infiltration of computers, addresses, and profiles without the knowledge of their owners and their use to obtain information and to distribute messages on the Internet.

A particularly good example of the dimensions of these threats are the revelations concerning the activities of the British consultation company Cambridge Analytica (CA), as well as concerning the role of the 'Facebook' social network in this process [Trud, Труд 31.03.2018];

B) Individually and socially, these threats become ever more tangible in relation to:

- the violations of the rights to privacy;
- the intrusions into the personal, including the intimate 'space' of individuals;
- the risks of 'identity thefts' and 'draining' of bank accounts;
- the danger of dissemination of discrediting, usually untrue and unverified information that undermines the public profiles of both individuals and various public institutions and organizations.

Social networks are now able not only to store and 'process' information available in cyberspace, but also to recover data that had already been destroyed as 'unwanted' from users, as well as to 'create' profiles themselves without asking for permission [Sega, Сега 11.04.2018].

C) The threats for the political processes are particularly alarming.

Anonymity in the virtual space is a prerequisite for the lack of control and the irresponsibility of its 'inhabitants'; the 'multi-personality' - for the impossibility of identifying the 'sources' of the information disseminated in the network; the speed of creating 'cyber-news' (on-line mode) – for the inability of the politically responsible subjects to control their credibility and to respond adequately; the accessibility - for the presence of various, including extremist and terrorist actors, messages and actions; the low prices and the lack of risks for the consumer - for the persistence in the messages sent and for 'lack of censoring' of their content; the liberalism and activism - for the limitlessness of the demands for freedom and independence.

POLITICS AND CYBER SECURITY IN THE COMMUNICATIONS SOCIETY

Policy in the Communication Society

The major political change resulting from the total cybernization of modern society consists in a 'rearrangement' of the structure and hierarchy of the political system and the mechanisms of political processes.

In modern society, including the 'information' society, the political hierarchy is characterized by a pronounced dominance of state power, particularly of the central state institutions.

However, the post-modern, communication society, is characterized by a contradictory process of 'pluralisation' or 'networking' of the power centers.

This phenomenon is, in the first place, related to the emergence of new 'virtual-real', political actors who are independent from the states and impose new forms of political action and organization of the political life as a whole.

The pluralisation also manifests itself as a 'pluralisation' of sovereignty, which, from the sole state power (head of state, parliament, government), is partially passed on to, or is 'appropriated' by, new subjects ('net communities', 'net Demos', 'Netocracy'), which significantly limits the capabilities of the state uncontrollably

A) to rule in the public domain;

B) to define the 'agenda' of society.

A manifestation of this change, for example, is the position of John Perry Barlow, the author of the famous 'Cyberspace Independence Statement', which, in its publicity to the participants in the 1996 Davos Forum, tells politicians: 'You are not needed any longer. You no longer have the supreme power where we have gathered. You do not have the moral right to rule over us, nor use the methods of compulsion that could scare us. You do not know us or our world. Cyberspace is beyond your borders.' [123.dir.bg/articles/free.htm; News. bg, 30.06.2012].

An important political outcome of this 'internalization' (especially in Web 2.0 and Web 3.0) is the elimination of the state monopoly in the information space which used to creat conditions allowing the state to impose a political ideology (and mythology) convenient for its domination, and an uncritical acceptance by the 'mass' of the state's decisions. This elimination of the state monopoly is evident from:

A) a noticeable spirit of criticism (often unlimited and insufficiently substantiated);

B) the alternative to offering and adopting political ideas, programs and models.

Great opportunities in this respect is the so-called 'Political blogosphere'. Political blogs bring together both the positions of leading political leaders and the opinions of the many ordinary users 'visiting' their blogs, which, in the opinion of the Wikipedia creator J. Wales, expressed in his 'Open Letter to the Political Blogosphere', makes the blogosphere a basis for 'the politics of the future' [Wales 1996].

The 'transition' of sovereignty to the new virtual reality entities of the communication society is particularly effective in that it allows the exrcise of a permanent control over state and political institutions and figures (instead of once every 2 or 4 years, during the elections).

In the context of modern digital technologies and the Internet, information about official political subjects is freely collected and disseminated, and its accessibility in the Internet puts political elites and empowered state institutions in a 'subordinate' position, forcing them to constantly take into account and respect the Internet community.

As Brian McNair points out in relation to the scandal concerning US President Bill Clinton's relationship with Monica Lewinsky, in the 'digitized' society, 'nothing remains hidden for long, and there is no such thing as "outside the record". Political actors must adapt to this new reality or perish under the pressure of hostile public opinion.' [Prodanov, Проданов, 2012].

A much more effective mechanism of pluralisation of the actors influencing the dynamics and direction of political life in digital society is the establishment of a new type of 'activism'.

It has many manifestations that can generally be grouped into two large groups:

A) activism 'implemented' inside cyberspace;

B) and activism emerging outside of cyberspace and flowing into the 'virtual-reality' communication society.

The first type covers activities of both qualified, specially prepared and ordinary network users related to specific political actions of the 'responsible' political subjects - governments, parliaments, political leaders. For these activities:

A) information on unpublicized or deliberately hidden intentions, prepared offenses etc. is disseminated on the Internet;

B) discussions are held on the issues raised and the published information is assessed;

C) a 'public' opinion supporting or rejecting the actions of the political institutions and of the virtual network users involved in the virtual dispute is formed.

Indisputable in this regard is the situation which arose around the disclosures made in the Wikileaks website created by Julian Assange about the work of US diplomats around the world.

The second major form of activism in the communications society is the unification through the social networks of virtual political actions with real ones in the modern virtual-real world, which has a significant impact on institutionalized political forces (most often governments) in their specific political and gvernmental activities.

From the point of view of their impact on security, the following features of this mergering are the most important:

A) the speed of formation and the often short-term accessibility;

B) the anonymity of participation;

C) the emergence of 'horizontal' relationships and interactions between individuals and groups in communities;

D) the lack of 'leadership';

E) the spontaneous emergence (usually on the occasion of a specific political act and the ‘retaliation’ in the ‘respondents’ network in the ‘real‘ socio-political space);

F) the self-organization and authenticity of participants.

One of the most striking manifestations of networking are ‘flash mobs’ that emerge almost instantly and bring together strangers in a given location to exercise pressure in order to achieve resolvement of various political problems or to protect the rights and interests of individual persons and (or) marginalized groups which would not be attainable by the traditional political means available in the modern political space.

Digital cyber-terrorism and cyberwar are other specific political manifestations of digital society. Cyber terrorism is a form of political terrorism (terrere: in Latin - to tremble, to fear) in the virtual real world. Cyber terrorism:

A) is the deliberate performance of cyber attacks against computer systems, networks, software and information by politically motivated individuals or collective subjects;

B) aims to bring bout their destruction, blocking, or interferences with their normal functioning;

C) creates an atmosphere of fear and insecurity in society;

D) forces the political authorities to take action to meet the demands made by cyber-terrorists [Tropina, Тропина, 2003].

Cyber terrorism finds realization in two basic forms:

The first one involves cyber attacks targeting computer systems, communications networks and the information platforms of political actors (governments, state institutions, parties, political leaders) aimed at achieving the political goals of terrorists. This form can also be defined as a distinctive virtual terrorism. (A recent example of virtual terrorism is the May 2017 cyber attack with the WannaCry virus, which affected consumers - mostly companies and state structures - from almost the whole world.)

The other form is related to the actions in ‘virtual-real’ reality, where the ‘ultimate’ objective of cyber attacks can be physical objects of real space, and terrorist operations can include a broader range of activities such as:

A) organization of terrorist groups and support through and in the virtual space;

B) advocacy and protection of their ideas, political platforms and demands;

C) providing funding for their activities;

D) creating a feeling of fear in the virtual and real world;

E) recruiting and training members of virtual and real terrorist groups and setting goals for their activities;

F) dissemination of information in the Internet space (including the so-called steganography, i.e. by sending messages to sites having totally different 'peaceful' content that can only be recognized and 'read' by the 'dedicated' users) which organizes and motivates terrorists politically and ideologically and ensures the fulfillment of the assigned tasks [Vayman, Вайман, 2012].

Cyberwar is difficult to distinguish from cyber terrorism, but constitutes a seperate form of 'cyber-violence' in the virtual world.

The following most important differences between cyber-terrorism and cyberwar may be identified:

A) the nature of cyber-attackers - in cyberwars, they are run by state structures (the USA and Russia have already established 'high commands' and cyber-warfare services), whereas in cyberterrorism they are led by 'independent' network users;

B) the goals set - in cyberwars, the aim is to achieve cyber-superiority and even destroy the cyber-structures and cyberpotential of the enemy, and ultimately to 'conquer' its virtual realities and to subordinate it to the military, political, economic demands and conditions of the winner.

The main difference is that, at least for now, cyberwar attacks are relatively rarer than cyber- terror attacks in the virtual and virtual real-time space.

Security in Communication Society

It follwos from what has been said about the political characteristics of the communication society that cyber security is one of the most important aspects of security and that whatever the state of cybersecurity determines the state of national security.

This conclusion is supported also by the position of former US President Barack Obama, expessed at the beginning of his term, that 'cyber-threats are one of the most serious challenges to the economy and national security faced by the US as a nation' and that 'America's prosperity in the 21st century will depend on its cybersecurity'.

Definition of security

The issues related to the essence of security and the mechanisms for achieving security have long been addressed by the socio-political thought, but they became the subject of special attention at the middle of the twentieth century.

In political science, security traditionally been associated with the functions of the state. In this sense, it is defined as 'state' or 'national' security.

Security is an irrevocable feature of statehood that manifests itself:

1) in the creation of a system of factors preventing external and internal conflicts;

2) in ensuring the protection of citizens and national wealth;

3) in preserving national sovereignty, territorial integrity and the stability of the state.

In this sense, national security is also addressed in the UN Charter where it is noted that it is a dynamic state in which there is no direct danger for society from armed aggression, political pressure or economic coercion so that the society may freely pursue its development.

Based on this perception of security, cybersecurity may be considered as a policy aimed at building a society that is capable of:

A) preventing threats and responding to them;

B) ensuring the superiority of the state in the virtual (cyber) space, in its building and operating by providing the necessary for that purpose:

- resources ('cyberpower');
- subjects ('cyber-specialists');
- institutional basis (state specialized bodies and legal and regulatory basis) security.

Cyber security has three main dimensions - technological, legal (institutional), an political.

In a technological plan, cybersecurity faces the need to find an adequate response to the attacks on computer systems and the Internet.

It should be pointed out in particular that with the development of information and communication technologies and their transformation into a decisive component of the communication society, cyber-attacks begin to take place under the control and protection and with the participation of a number of 'official' subjects - state and non-state institutions, business organizations and companies that attract cybersecurity experts. So-called experts are most often hackers (crackers) who perform cyber-security breakthroughs in hostile states or their organizations (army, security services, critical infrastructure authorities), in order to hamper the activity of the competition or to retrieve information about it. Thus, technological threats greatly expand their reach and tend to escalate considerably, which makes it primary task for states take action to prevent them.

In general, action can be taken at three levels: at the level of an ordinary user; at the level of providers of computer systems, software and internet; and at the level of state regulation of cyberspace. The latter level is the most important one from the point of view of national security.

Ordinary internet users can protect themselves from malicious software by being aware of it, by installing security software (antivirus), and by regularly updating it. Scanning the system also increases the level of protection. To increase the level of protection of a personal computer, it is advisable to install a firewall as well. Firewalls provide protection by filtering the information and then, after having analyzed it, by authorizing or prohibiting its transmission.

On the second level, security is far more difficult to achieve. The three rules formulated by Peter Lindstrom - an expert from Burton Group, in his publication, outline an issue related to the protection of the virtual environment: that all known operating system attacks use the same template. There are different so-called cyber-security architectures, namely a set of measures that cover the tactical, strategic and operational levels. One of them is the SANS architecture, also known as "20 Critical Security Controls," which sets out ways to measure and test the applied measures and tools, and an example scheme for inter-state relationships that address the use of this type of vulnerabilities. These ways are formulated in the twenty security controls, and the architecture of Northrop Grumman Corp includes five security layers [Стоянов, Геов / Stoyanov, Geov (2013)]:

1. Perimeter security
2. Network security
3. Security at the endpoints
4. Application security

5. Data security

As a conclusion related to this level, it can be said that the increasing number of dangers endangering cybersecurity justifies the current emergence of systems of technologies developed to achieve cybersecurity. In order to achieve a good level of protection, a significant amount of resources should be invested and a comsiderable attention should be paid to every detail - from the site's foundation to the latest news about virtual security. The technology of guaranteeing cybersecurity has not yet been sufficiently developed. In future, with the expected modernization and globalization, this problem will become even more pressing.

The third level of technological security is state regulation. Liquidating cybercrimes is of the utmost importance for the achievement of national security. Cyberspace is a critical infrastructure due to the fact that a disruption of the status quo may permanently affect the life of the individual and the society as a whole, and it is precisely for this reason that modern states, particularly the most technologically advanced among them, take special complex measures to regulate cyberspace. After the cyber attacks against Estonia in 2007 and Georgia in 2008, the USA performed a comprehensive Cyberspace Policy Preview, followed by the adoption of the Comprehensive National Cybersecurity Initiative. Appropriate institutional reforms are also under way in the US, such as the appointment of a Cyber Security Coordinator and the establishment of a Cyber Security Office within the National Security Staff. More than 500 legislative acts on cybercrime and data protection are currently in place in the USA [Grancharov, Грънчаров 2011].

Since 2005, NATO has taken not of the exceptional importance of cybersecurity and has been actively involved in this field. The impetus for active action came after the attacks on the information systems in Estonia and Georgia, with the establishment of NATO Cyber Defense Management Authorities (NATO CDMA), as well as of a NATO Centre of excellence.

In 2003, the European Parliament adopted a regulation establishing a European Network and Information Security Agency (ENISA). The Agency started working in 2005 and aims to strengthen the network and information security in Europe and the ability of Member States, both individually and concertedly, to address the major network and information security issues.

For each state, the Agency prepares a report that provides information on network and information security issues [Kuzmanov, Кузманов 2011].

There are two main problems related to the legal aspects of security in the virtual space: 1) the need of an elaboration of a legal framework of the virtual space; and 2) the definition, identification and combatting of cybercrimes.

The term 'computer crimes' first appeared in scientific literature in the 1960's [Dimitrov Димитров 2008], after some cases of illegal use of computer systems, computer sabotage and computer espionage were revealed. More in-depth analyzes of this kind of crimes began in the 1970s. Approximately at the same time, in a number of states, special data protection legislation was adopted sanctioning the infringements related to personal data that was electronically collected, stored and transmitted. From a historical point of view, these are the first legislative provisions in this area. In most cases, traditional criminal legislation turns out to be inapplicable to such crimes which requires international cooperation. New trends in the development of cyberspace legislation became noticeable in the 1990s, when computer crimes began to affect an ever larger circle of public relations: the spheres of state government, healthcare, transport etc. The rapid pace of Internet development as a global network gave rise to new and serious challenges for many states in the field of criminal policy. Information systems have been turned into tools for criminal activity by organized crime groups, which poses great risks to national and international security and thus boosts international cooperation in the field of digital security. Separate states have adopted a number of new regulations and are launching international initiatives aimed at unifying the internal regulation and at establishing effective mechanisms for international cooperation.

Ever more active efforts have been made in recent decades to elaborate an international legal framework aimed at combatting cybercrimes. The Council of Europe has adopted a number of important instruments in the fight against crimes committed through the use of computer systems and networks or electronic information, as well as by their abuse.

A special challenge for the legal framework is to come up with a definition of the term 'computer crime'. 'Cybercrimes' ('computer crimes', 'computer-related crimes' or 'high technology crimes') should be understood as 'criminal offenses carried out through the use of electronic communications networks and information systems or against such networks and systems'. In fact, the concept refers to three categories of criminal acts occurring in the virtual-real space. The first encompasses traditional types of crime such as fraud or forgery, but in the context of cybercrime, this category refers in particular to crimes of this type committed through electronic communications networks and information systems ('electronic networks'). The second concerns the publishing in the electronic media of illegal content (eg. child pornography or materials aimed at increasing racial hatred). The third category of crimes includes such crimes that are unique to electronic networks, for example attacks against information systems, denial of service and unauthorized access (hacking) [http://library.netlaw.bg/l_bg/?s=1].

In June 2001, the Convention on Cybercrime was adopted. The Convention contains a legal framework dividing the offences into four major categories, namely:

- offenses related to the confidentiality, security and access to data and information systems: unauthorized access, illegal interception, infringements of the data protection rules, intrusion, device misuse;
- computer crimes: computer forgery and computer fraud;
- content-related offenses: the production, distribution and possession of child pornography;
- offenses related to copyright and related rights: mass distribution of illicit copies of copyrighted works on a large scale.

Political Security in Communication Society

The achievement of cybersecurity is related to the building a brand 'new architecture' as compared to the national security systems typical of the 'modern' society as a whole.

The starting point for the establishment of the new security architecture is the reinforcement of the understanding that the main objective of cybersecurity is to eliminate the threats to the sovereignty of the state (of the central political power) in the virtual and virtual-real space, both internally and internationally.

The achievement of this goal is related to the undertaking of actions aimed at achieving a 'cyberpower' monopoly in the communication society, which would lead to cyber stability, cyber governance and cyber-dominance which in turn would ensure the protection of national interests and the sustainable functioning and development of state and society.

There are several main political directions for the realization of these security objectives in the digital world.

In the first place, these are actions aimed at limiting or eliminating the 'specifics' of the virtual-real reality, and in particular:

A) the limitation of access and presence on the Internet;

B) the subjective and ideological pluralism;

C) the anonymity;

D) the lack of responsibility.

Depending on the specific conditions and character of the political regimes in individual states, the actions taken may have a number of peculiarities, but generally they include mainly:

A) narrowing the scope of virtual space by regulating access to certain sites, platforms, Internet services;

B) restriction and centralization of Internet operators and providers with the aim of ensuring their minimization and the exercise of state control over them.

As E. Schmidt, a former Google CEO and a member of the Council of Science and Technology during the rule of US President Barack Obama, has pointed out, an indication of the "efficiency' of these mechanisms is the fact that in a number of states, particularly the states from BRICS and China and Russia, as well as Iran, digital technologies are perceived as a powerful modern means of strengthening existing political regimes. According to him, 'probably no country has considered more carefully the consequences of giving free access to citizens to technologies that may connect them, than has China. The objectives of the regime are clear: to control the access to content on the Internet and to use technology to build its own political and economic power. Beijing arrests online activists and uses highly developed bulletin boards to broaden its propaganda. All this is part of a strategy that should make ensure that the technological revolution strengthens, rather than destroy the one-party state and its system. All over the world, the Chinese Internet control model is being copied by other states such as Vietnam and is being actively popularized in Asian and African countries where China is investing heavily in natural resources. In addition, Beijing is actively penetrating international institutions, such as the International Telecommunication Union, to imrpove its image and gain trust worldwide and to finde allies in its attempts of controlling the telecommunications of it citizens". [Shmid, Шмид - 2011].

The second important form is to control the content of the information on the web by:

A) manipulation of information flows and inclusion of 'pseudo' virtual subjects (sources of information and users) behind whom there are specialized state services, the creation of specialized bodies, and the development of virtual-real space tracking systems to identify the real and virtual subjects involved in 'active' illegal actions. Particularly active in this respect, for example, are a number of US government services. As stated in an article published in Computerworld, if judging by the Internet queries done by federal law enforcement and intelligence agencies triggered by the events during the Arab Spring, the US government is looking for a software capable of tracking social networks to predict all sorts of things - from future terrorist attacks to foreign uprisings. The system they dream of in the National Intelligence Research Unit would merge everything - from web search engines through Wikipedia articles to automotive surveillance cameras in order to 'overtake the news' by anticipating important events - from economic chaos to epidemics. The Department of Defense's program, for its part, will be able to monitor social media to detect the dissemination of information that could affect soldiers on the battlefield, but also to enable the military to perform their own 'operations fof influence' in social media to counteract enemy campaigns. Another important goal of the services is to play with the 'authenticity' of the information that is to be found in social networks. Computer programs, known as bots, are already infecting social media such as Twitter with useless posts similar to spam-emails. This plays an important role in gathering intelligence, because bots may mislead independent analysts (and their software) to believe there has been a real change in social attitudes, while in fact the shift they notice may be a government propaganda campaign, carried out, for example, by Twitter users that do not exist at all [Computerworld, 08.12.2010].

B) Creating specialized bodies and building systems for 'tracking' in the virtual real world which reveal the identity of the 'active' virtual and real subjects participating in 'active' anti -government actions. This creates conditions for 'kickbacks' on activists to provoke fear of retribution and for them touse ref to participate in anti-government actions. A typical example of the efficiency of the use of the 'duality' of the virtual space are the actions of the Iranian authorities during the 2009 presidential election when, in order to 'intimidate' the supporters of the opposition, the security services not only monitored internet 'trafficking' through which the protests were organized and directed, but also participated in it by sending their own messages to the protesters intended to reveal their personal identification and speading pro-governmental content, including threats of prosecution. Similar actions were taken by the Turkish authorities in protests at Tahrir Square in 2013.

The third main strand is the development of stand-alone cyber security policies in the national security system of the modern state.

A key element of cybersecurity policy is the development of a political and legal framework for its implementation in the modern communication society and the building of this technological and organizational structure which makes it possible to implement it in virtual-real space.

Other important steps of the NATO's policy in this regard are for instance:

A) NATO's Cybersecurity Policy adopted in February 2008 in Bucharest;

B) NATO's concept of cyber-security approved in April 2008.

The European Union, for its part, as already indicated above, created in 2005 the European Network and Information Security Agency (ENISA) [Ivanov, Иванов, 2011].

A second major component of cybersecurity policy is to take concrete action for its implementation in the life of society by:

A) training and upskilling of staff, conducting 'training' similar to traditional military training but simulating cyber attacks: An expression of this need are the actions that the EU and NATO took after the cyber attack in 2007 against Estonia, which effectively blocked the activities of the government and the state as a whole for almost three days. These measures of the EU and NATO consist in paying special attention to the prevention and response to cyberattacks, including by conducting large-scale 'cyber-trainings'. In Estonia trainings are run annually under the leadership of the Cyber Desense League (CDL). Even during the very first such teaching that took place in 2010, Locked Shields ten teams defended a pre-established virtual network. As Leina Areng, a cyber security adviser at the Estonian Ministry of Defense points out, 'a year earlier' a list of 'all companies which are critical to society' was prepared and '42 services that have vital importance and can be the subject the cyber-attack' were listed. All these governmental structures and companies must report to the Estonian Information System's Authority (EISA) in the event of an incident. Such 'exercises' are also being conducted within NATO, as well as by the USA Army and the USA Security Authorities, which in 2010 conducted the first major exercise under the new Plan for Defense against Cyberattacks, including attacks on energy, water and banking systems [Ivanov, Иванов, 2011].

B) implementing counter-actions to prevent and/or limit damages and to restore the integrit of the 'national' cyberspace: The objectives of the above mentioned actions are to improve the cyber-attack preparadaness and to examine the responses in case of incidents and the exchange of information between the different political and defense institutions and authorities, international organizations and private partners. In essence, these measures are aimed at 'achieving sustainability' and at enhancing the 'nation's ability to cope with the loss of or damage inflicted upon key aspects of modern life', as stated in a statement by the National Cyber Security and Communication Integration Center at the Department of Homeland Security [Milev, Милев, 2010].

The creation and deployment of a new kind of armed forces 'cyber' troops is relatively self-directed. These 'cyber' troops are built to be able to lead cyberwar in all directions:

A) intelligence (espionage)

The revelations done by the former CIA agent Edward Snowden speek volumes about the scale and consistency of the 'intelligence operations' performed in cyberspace. From the data disclosed by Snowden, as well as from several others scources which leeked information after the scandal broke out, it became apparent that the US security services, and in particular the National Security Agency, had worked in 'close cooperation' with Microsoft, Yahoo, Google, Facebook, Skype, YouTube, Apple, having had direct access to their main servers and having received Internet traffic information from them, not only about 'enemy' but also about 'friendly' governments [Trud, Trud, April 12, 2018]. It should be pointed out, however, that such actions are common practice in international politics and are being currently used not only by the US intelligence services but also by their closest allies in

NATO, as is the case with the Directorate General for External Security of France (DGSE), which has completely listened to all communications that it had been able to access and has been storing such communications for years [Sega, **Сега, 13.07.2013**].

Mutual accusations of 'electronic' espionage have become one of the most significant manifestations of the ever-increasing conuction of a 'new' cold war between the USA and Russia, as well as between the West and the East as a whole. Such accusations reached their peak after the election of the current US president Donald Trump when the Democratic Party that had lost the elections spread the opinion that one of the main reasons for Trump's victory had been the performance of cyber attacks by Russian 'governmental hackers' supporting the Republican candidate. It is alleged that the US secret services have evidence that Russian hackers with the approval of the Kremlin have infiltrated the Democratic Party's computer system and have distributed domestic e-mail. The FBI has presented a report with the technical characteristics of the hacker attacks. The document provides details on the attacks performed under the code name 'Grizzly Steppe' according to which since the mid-2015 the Russian foreign intelligence has been sending emails with viruses to over 1,000 US citizens, including government officials. Internal sources say the FBI report confirms to a large extent the already released disclosures of private security companies. [www.transmedia.bg/2016/12/31].

B) Preventing or neutralizing enemy cyber attacks;

Attacking, crushing its cyber-protection and 'cyber-powers' and securing victory in the war.

An example of concrete actions aimed at preparing for cyber wars is the Pentagon's position that the first battle in the wars of the future will be the battle 'for control over the so-called cyberspace' as 'if we do not control cyberspace, we can not controll the air, the space, the maritime space and our territory'. An expression of this position is the building of structures in the US Armed Forces counting a staff of 40,000. [Nikolov, Николов, 2009]. The administration of current US President Donald Trump has brought forward the formation of 'cyber powers' and the increase in the costs needed for their development.

An indicator of this trend is the fact that if in the 2016 budget the proposed 14 billion dollars for cybersecurity were only 1 billion more than in 2015, the 2017 growth in comparison to 2016 is nearly 7 billion and reaches an impressive overall amount of nearly 21 billion. A special group of 5,000 people is already ready for action in key areas, with a further 1,200 specialists expected to join it in the next two years. They will join the already existing army of 40,000 employees who are engaged in both digital intelligence and in performing destructive attacks on enemy computer networks. These troops are deployed in all types of US Armed Forces - infantry, fleet, air forces, and landing units that already have their own cyber-divisions, which is an indication of the advanced stage of the US cyberwar-preparation. Until now, governmental cyber-operations have been conducted by various organizations - the NSA, the Pentagon Cyber Command and other military agencies. The current administration intends for centralize the actions and to reduce the bureaucratic procedures [Shopov, Шопов 2017].

Russia, for its part, has also set up a new generation of troops responsible for the country's cyber security [btvnews.bg, 05.07.2013]. The newly-formed Russian Armed Cyber forces aim to protect national security by opposing any attacks made on cyberspace. However, they may also be used for offensive purposes. According to Defense Minister Sergei Shoigu, this army will be very effective and powerful [Standart Nyuz, Standard News, 22.02.2017, www.standartnews.com]. These forces have their own command within the structure of the armed forces and, despite some falling behind, will soon be provided with the most up-to-date equipment up to the lowest of ranks. For example, it is believed that advanced computers with robust anti-hacker protection are now available to the Russian armed forces' tactical squadrons to protect vital information from spies. According to information provided by the United Instrument-Building Corporation, a portable computer has been introduced in the Russian Army which works with an Astra Linux operating system and ensures maximum protection against cyber-attacks and data leakage, including during the transmission of text, voice and video messages [Infobalkani, (2016)].

CONCLUSION

In conclusion, it can be said that the features and characteristics of security in the virtual real world that have been outlined so far help to define the 'limit' in its achievement in socital practice as a major problem.

The reasons for the existence of the problem of cybersecurity are mainly related to:

A) the contradictory nature of the interests and objectives of the subjects in the communication society;

B) and their desire to achieve unilateral superiority in the protection and realization of these interests and goals.

As a result, actions are taken internally which lead not only to protecting the security of cyberspace but also to limiting the freedom in it, including some instances where a kind of 'cyber- dictatorships' have been imposed.

Under the pretext of combatting 'cyber terrorism' and the threats of anarchy in the virtual-real world governments take action that leads to the establishment of a total monopoly in the digital society - from cyber-pending to the adoption of laws incriminating actions of Internet users that are 'unacceptable' from the point of view of security.

The directive adopted by the European Parliament on the application of tougher sanctions against cyber-attackers, is, in the opinion of technology blogger Glin Moody expressed on Twitter, 'intimidating' because it is very likely 'that EU governments are abusing the laws and prosecuting programmers and techno-maniacs'. This, in his view, is the way to make reality the profound predictions of J. Orwell's '1984' anti-utopia and to realize the dreams of all 'totalitarians', from Plato and the Inquisition, Hitler and Stalin, to the Big Brother of digital society, of destroying individual freedom of [Computerworld, 05.06.2013; isocbg.wordpress.com/2009/; Stamenov, Utsan, Стаменов, Утсън, 2010].

From the point of view of foreign policy, the pursuit of 'security' in cyberspace is related to the development of a steadily expanding spiral of actions to achieve domination in the virtual-real world, which not only does not increase but, on the contrary, reduces the security of digital society. The increase in 'power' on one side leads to retaliatory measures of the other, etc.

It is clear that today's world - the virtual-real world of the 21st century – will have to overcome big challenges – a big 'risk' - and one of the possible ways of achieving that is by studying and identifying the manifestations of this 'risk', in order to thus be able to outline the essence and the characteristics of cybersecurity, which was also the goal of this paper.

REFERENCES

Бек, У. (2001), Световното рисково общество, Обсидиан, София.

БиТиВи Нюз (2013). Русия създава кибер-подразделения в армията, btvnews.bg, 05.07.2013.

Вайман, Г., Внимание терористи дебнат в социалните мрежи, Glasove, www.glasove.com/vnimanie-teroristi-debnat-v-sotsialnite-mrezhi--20295, 07.04.2012.

Велкова, Л., и др. (2012), За еволюцията на понятието "сигурност", Аспекти на сигурността, София, с. 39-40.

Грънчаров, В. (2011), Държавната политика по защита на информацията в началото на 21 век, Проблеми на информационната сигурност през XXI век, Шумен.

Димитров, Г., (2008). Правосъдието в дигиталната ера: Аналитичен доклад, Law and Foundation, Justice in the Digital Era Project, Analytical Report BG, София.

Иванов, И., (2011). Киберзащитата – приоритет на Алианса, Проблеми на информационната сигурност през XXI в., Шумен.

Инфобалкани, (2016). Оборудват руската армия с компютри с непробиваема кибер защита, Инфобалкани, https://infobalkani.wordpress.com/2016/02/19

Компютъруърлд, (2010). Разузнавателните служби на САЩ ровят в социалните мрежи в търсене на прогнози за бъдещето, Computerworld, 08.12.2010

Кузманов З., (2011). Заплахи за критичната инфраструктура в електроенергийния сектор и информационните и коминикационните технологии, Проблеми на информационната сигурност през XXI век, Шумен.

Милев, М. (2012), От Хакервил до киберфронта, Капитал, 5.10.2012.

Николов, С. (2009), Направления за развитие на научните изследвания в областта на отбраната и сигурността, Център за стратегически изследвания в сигурността и международните отношения, csr-bg.com/archiv_1/badesti_woini.htm.

Проданов, Х. (2012), Дигиталната политика, Фабер, София.

Сега, (2013). Майкрософт помагал на властите в САЩ да шпионират, Сега, 13.07.2013.

Сега, (2018). Фейсбук ни следи и без да сме в мрежата; Ю Тюб е обвинена, че незаконно прави профили на деца, Сега, 11.04.2018.

Стаменов, И., С. Утсън (2010), Бавното убийство на свободния интернет, Hi Come, м. септември.

Стандарт Нюз, (2016). Русия се похвали с кибер войска, Стандарт Нюз, 22.02.2017, www.standartnews.com

Становище, (2009). Становище на „Интернет общество – България“ по Законопроекта за изменение и допълнение на ЗЕС и мотивите към него, предоставени за публично обсъждане от МВР, isocbg.wordpress.com/2009/.

Стоянов, Н., А. Геов (2013). Архитектура за киберсигурност – технологични аспекти, cio.bg, http://www.cio.bg/5603_arhitektura_za_kibersigurnost_tehnologichni_aspekti.

Трансмедия, (2016). САЩ и Русия в спиралата на Студената война, www.transmedia.bg/2016/12/31

Тропина, Т. (2003), Киберпреступность и кибертерроризм, Киев, ndki.narod.ru/.../Tropina_TL-Definitions1.doc

Труд, (2018a). Вижте всички данни, които Facebook и Google имат за вас, Труд 31.03.2018.

Труд, (2018b). Фейсбук водел оръжейна надпревара с руснаците, Труд, 12.04.2018.

Фондация „Право и Интернет“ - http://library.netlaw.bg/l_bg/?s=1

Шмид, Е., (2011). Дигиталният пробив, Либерален преглед, http//www.librev.com/index.php.

Шопов, М., (2017). Война или мир в киберпространството, Нова зора, 14.07.2017, www.zora-news.com/index.php?option=com_content&view=article.

Bek, U. (2001), Svetovnoto riskovo obshtestvo, Sofia, Obsidian.

BTV News (2013). Rusia sazdava kiber-podrazdeleniya v armiyata, btvnews.bg, 05.07.2013.

Computerworld, (2010). Razuznavatelnite sluzhbi na SASHT rovyat v sotsialnite mrezhi v tarsene na prognozi za badeshteto, Computerworld, 08.12.2010.

Computerworld, 05.06.2013.

Dimitrov, G., (2008). Pravosadieto v digitalnata era; Analitichen doklad, Law and Foundation, Justice in the Digital Era Project, Analytical Report BG, Sofia.

Grancharov, V., (2011). Darzhavnata politika po zashtita na informatsiyata v nachaloto na 21 vek, Problemi na informatsionnata sigurnost prez XXI vek, Shumen.

Infobalkani, (2016). Oborudvat ruskata armiya s kompyutri s neprobivaema kiber zashtita, Infobalkani, https://infobalkani.wordpress.com/2016/.

Ivanov, I., (2011). Kiberzashtitata – prioritet na Aliansa. Problemi na informatsionnata sigurnost prez XXI v., Shumen.

Kuzmanov Z., (2011). Zaplahi za kritichnata infrastruktura v elektroenergiyniya sektor i informatsionnite i kominikatsionnite tehnologii, Problemi na informatsionnata sigurnost prez XXI vek, Shumen.

Law and Internet Foundation - http://library.netlaw.bg/l_en/?s=1.

Milev, M., (2012). Ot Hakervil do kiberfronta, Kapital, 5.10.2012.

News.bg, 30.06.2012.

News.bg, 22.10.2012.

Nikolov, S. (2009), Napravleniya za razvitie na nauchnite izsledvaniya v oblastta na otbranata i sigurnostta, Center for strategic research in the field of security and international relations, csr-bg.com/archiv_1/badesti_woini.htm.

Prodanov, H., (2012). Digitalnata politika, Faber, Sofia.

Sega, (2013). Maykrosoft pomagal na vlastite v SASHT da shpionirat, Sega, 13.07.2013.

Sega, (2018). Facebook ni sledi i bez da sme v mrezhata; YouTube e obvinena, che nezakonno pravi profili na detsa, Sega, 11.04.2018.

Shmid, E., (2011). Digitalniyat probiv, Liberalen pregled, http//www.librev.com/index.php.

Shopov, M., (2017). Voyna ili mir v kiberprostranstvoto, Nova zora, 14.07.2017, www.zora-news.com/index.php?option=com_content&view=article.

Stamenov, I., S. Utsan (2010), Bavnoto ubiystvo na svobodniya internet, Hi Come, September.

Standart News, (2017). Rusia se pohvali s kiber voyska, Standartnews, 22.02.2017 www.standartnews.com.

Stanovishte, (2009). Stanovishte na „Internet obshtestvo – Balgariya“ po Zakonoproekta za izmenenie i dopalnenie na ZES i motivite kam nego, predostaveni za publichno obsazhdane ot MVR, isocbg.wordpress.com/2009/.

Stoyanov, N., A. Geov (2013). Arhitektura za kibersigurnost - tehnologichni aspekti, cio.bg, http://www.cio.bg/5603_arhitektura_za_kibersigurnost_tehnologichni_aspekti.

Transmedia, (2016). SASHT i Rusiya v spiralata na Studenata voyna, Transmedia, www.transmedia.bg/2016/12/31.

Tropina, T. (2003), Kiberprestupnosty i kiberterrorizm, Kiev, ndki.narod.ru/.../Tropina_TLDefinitions1.doc.

Trud, (2018a). Facebook vodel orazheyna nadprevara s rusnatsite, Trud, 31.03.2018.

Trud, (2018b). Vizhte vsichki danni, koito Facebook i Google imat za vas, Sega, 11.04.2018.

Vayman, G., (2012). Vnimanie teroristi debnat v sotsialnite mrezhi, Glasove, 07.04.2012, www.glasove.com/vnimanieteroristi-debnat-v-sotsialnite-mrezhi--20295.

Velkova, L., i dr. (2012), Za evolyutsiyata na ponyatieto “sigurnost”. Aspekti na sigurnostta, Sofia, pp. 39-40.

Wales, J., (2006). An open letter to the political blogosphere, http://campaigns.wikia.com/wiki/Mission Statement.

123.dir.bg/articles/free.htm.

UDC 343.9.02

ORGANIZED CRIME THREATS TO CORPORATE SECURITY

PhD Tanja Miloshevska[1], PhD Oliver Bakreski[2]

The purpose of this paper is to present how transnational organized crime threatens individuals, corporations, governments, and entire industries, undermining security, privacy, safety, and social order. In an age of globalization, it has adapted, forging new networks that cross cultures, language barriers, and international borders. Transnational organized crime is now widely recognized as a significant threat to both national and international security, and it threatens the integrity of our political and economic institutions everywhere. As a result of these changes, organised crime has become a pervasive and ubiquitous threat for businesses requiring a new response. The questions posed in this paper are: What are the implications for business? What can the private sector do to better protect its personnel, its products, and its customers? The new threat environment has changed the profession of corporate security managers too, widening the agenda and increasing the importance of the corporate security profile in organizations.

INTRODUCTION

Compared to public policing, private contract security, and national security in criminology, sociology, political science, history, and other disciplines in recent years, corporate security has received little attention. This

[1] Cc Cyril and Methodius University, Skopje, Institute for Security, Defence and Peace, e-mail: tanja@fzf.ukim.edu.mk

[2] Cc Cyril and Methodius University, Skopje, Institute for Security, Defence and Peace, e-mail: oliverbakreski@yahoo.com

neglect is surprising not only because corporate security has been operating in various organizations for decades, but furthermore because it is emerging as the primary form of security of the 21st century. This is evident by its ostensibly rapid spread and ambitious, even breath-taking governing aims. As the world is becoming more corporatized, corporate security is becoming more pervasive and powerful than ever before, significantly affecting the lives and property of those in and outside the large organizations in which it flourishes. It may soon be the case that all we will need to know, question, fear, or plan about security will be present in the corporate security realm [Walby & Lippert, 2004].

Organized crime, both national and cross border, is better understood as a mechanism fuelled by much the same factors as those that expand trade and development, communication, infrastructure, and health. This is evident at any level of crime, from pickpocketing to counterfeiting, shoplifting to money laundering. Where there is a demand, there is traditionally a supply, and criminal syndicates worldwide continue to find loopholes to raise profit via illegal means. Thus the term organized crime encompasses a wide range of national and transnational illegal activity that jeopardizes the economic and political stability of societies, in addition to posing a direct threat to life and development.

While law enforcement agencies—local, national, and international—continue to increase and improve their efforts to protect citizens against the ever-evolving nature of serious organized crime, there is also an increasing need for corporations to take a proactive, intelligence-led approach to protect their operations, assets, and integrity. Corporate security is responsible for coordinating the overall security of a corporation in close coordination with the business management and all the functions that are concerned with security, safety, business continuity, and compliance to safeguard business interests, people, profits, and reputation and mitigate risks. It is also responsible for guiding all employees into doing their part in the security system through their everyday actions and judgments. Apart from dealing with traditional security areas such as physical, technical, and human elements of securing people and property, corporate security incorporates information security, business continuity, and disaster recovery through the entire lifecycle of products and business processes to provide actual support in achieving business goals.

The aim of this chapter in monography is therefore to review the challenges that serious organized crime poses to the growth, development, and reputation of corporations and to examine the role of an effective intelligence-led approach to detecting, preventing, combating, and mitigating such activities.

THE CORPORATE SECURITY ENVIRONMENT

The security organization today is shaped by many influences. The specific needs, concerns, and vulnerabilities of a company; the capabilities of its security team; and the perception of management as to the value of security all contribute to the organization's structure and role. Even business downsizing trends influence the role of security. Because downsizing affects all aspects of business, security too has to learn to operate in a leaner environment with greater demands and higher expectations, while at the same time working in an environment of increased threats and risks. The challenges to the corporate security managers and security staff are ever increasing [Kovacich & Halibozek, 2003].

Whatever it's legal and material characteristics, any company taking risks in commercial competition has vulnerabilities in relation to its competitors, employees and customers. The need to ensure the organization's survival in the face of damages from natural disasters, economic, political or social risks and ensure the safety nets required by insurers and external regulations (employment and fire safety) creates very different perceptions and concerns in its leadership. Size, geographical location and business sector are three of the most significant macro-sociological variables necessary to comprehend the nature of the mechanisms used to protect against the vulnerabilities, risks and threats that affect businesses. In order to understand the internal protections found in large corporations in the era of global security—a new necessity for the science of policing as well as policing agencies—boldness as well as modesty will be required [Ocqueteau, 2011].

The security operating environment of the twenty-first century presents a wide range of challenges to organizations. Traditional physical threats have been supplemented and, in some cases, supplanted by rapidly evolving electronic threats, and the boundaries of the enterprise have become ever harder to define. Moreover, as HSBC (Hongkong and Shanghai Banking Corporation) is fond of declaring in its advertising, in the future, even the smallest companies will operate globally. Ultimately, business is all about pricing risk, and in this regard, security risks are no different than any other. This chapter therefore discusses some of the main operating threats to companies. There are of course others, but the areas outlined here are the ones that corporate security intelligence departments tend to focus time and effort on. In outline, these are as follows:

- Geopolitical risk
- Terrorism
- Cyber issues
- „Traditional" espionage and insider threats
- Single-issue activism
- Crime, including fraud and counterfeiting.

The new threat environment has changed the profession of corporate security managers too, widening the agenda and increasing the importance of the corporate security profile in organizations. In principle, many threats could be considered 'corporate security' issues. This is also true of those previously considered national security concerns to be dealt with at the state level. Corporate managers constantly select which security threats to act upon, which to take responsibility for and thus which can be defended as 'corporate.' [Walby & Lippert, 2014].

A key driver of 21st-century corporate security growth is 'responsibilization'and the embracing of the corporate environment by government as a whole of community response to national security threats, such as terrorism and transnational organized crime [Petersen, 2013].

Corporate security is a part of the security domain; however, it is not part of the private security sector [Brooks, 2014]. As Cubbage and Brooks [2012] state: 'Corporate Security is a unique . . . support function that for efficacy aligns with its corporation and assists in its success.' Private security provides goods and services to a third party. But corporate security is embedded in the organization itself, exploiting as required the other elements of the private security industry. For example, corporate security from time to time will employ the services of private security for guarding and response services. In addition, they may use the electronic security sector for the maintenance of closed-circuit television (CCTV) surveillance and access control. Corporate security operates across diverse areas of practice, such as public municipal government departments and private corporations, from small to large.

Justification of the corporate security function may be considered in either a neoliberal or a neo-republican view.

The neoliberal form attempts to tap into the traditional market logic, making security a matter of calculation and profits. The neoliberalists focus on demonstrating the security value-add, for example, managing loss control in a supply line.

In contrast, the neo-republican form of governance expresses an organic vision of a shared security responsibility, a common moral that 'we' are able to embrace contradictions between national security and business [Petersen, 2013:223]. Notwithstanding the neoliberal and neorepublican views of corporate security, responsibilization and control must also be considered.

Corporate security is in charge of analyzing and quantifying risks; inventing, planning, setting, and controlling security measures; and measuring the performance and success of security measures to predict and notice trends, prevent and stop incidents, and understand their correlation in diverse parts of the corporation and in different phases of business processes [Cabric, 2015].

The following activities are the main possible pillars of a corporate security function in the second decade of this century:

- Physical protection of assets
- Physical protection of people
- Business continuity
- Crisis response/management
- Cyber security
- Information and data protection
- Internal investigations
- Countering fraud and money laundering
- Counterespionage
- Brand protection
- Anti-counterfeiting/piracy

To do this effectively, the corporate security managers must consider the following:

- ✓ Demographic issues such as crime and the general security condition of the geographic area the target company operates within
- ✓ Business affiliations: Does the company have any risky relationships with companies or individuals? Is there any involvement in corrupt or criminal activities? It may be necessary to conduct a background investigation on the key persons to determine the following:
- ✓ Personal and business reputation of the target company and its executives.
- ✓ Criminal record or associations of key executives.
- ✓ Pending and threatened litigation against the company.
- ✓ Political affiliations and patronage of the company.
- ✓ Financial profile and lifestyle of key executives.
- ✓ Media image of the company and its key executives [Kovacich & Halibozek, 2003].

The most elaborate of recent attempts is based on the strategic paradigm of *detection, study and training regarding resilience to risk and threat.* For example, Yves Roucaute [Roucaute, 2010] suggests a hierarchy of threats ("processes induced by the human will"), expressing them in the following rhetoric of war:

- the scope of high intensity conflicts and attacks by *malevolent, fragile or failed states* trying to attack computer networks in order to destroy infrastructure;

- then, threats from *asymmetric warfare,* such as those embodied in radical Islam, terrorism or organized crime;

- threats connected to *soft power* seeking to undermine the authority, legality and legitimacy of a state, a government and the culture of a nation;

- Finally, threats related to cyber-attacks aimed at individuals, executives, businesses or a whole country. Implicit in this expertise is an assumption that is generally behaviourist: the malevolent threat explains protective behaviour that occurs, without consideration, except in the form of lip service, of a collective responsibility. It resonates with an emerging economy of private security, even of the privatization of security. In this scheme of thought, the range and number of threats and challenges is based on the size of the companies, the largest being considered as the most innovative in protective measures, whether they rely on internal mechanisms or external service providers through which they, as mature participants, shape the market. [Hassis & Masraff, 2010].

THREATS TO CORPORATE SECURITY FROM ORGANIZED CRIME GROUPS

Today, organized crime is one of the major threats to development and security. Often considered the “dark side” of globalisation, transnational crime is capitalizing on the expansion of international trade and is broadening its range of activity. Acting as multinational corporations, criminal groups seek profit through the evaluation of countries’ risks, benefits and markets analysis. The ability to constantly adapt to the changes at local and international levels, to create transnational networks and diversify activities in order to maximize the potential offered by globalisation are the main obstacles for all entities fighting organized crime. Further, the lack of judicial and enforcement tools plays a strategic role in the growth of criminal syndicates’ management of trafficking drugs, arms, human beings, counterfeiting and money laundering.

To make matters worse, globalization has allowed previously local criminal gangs and organizations to expand and cross national boundaries, creating a convergence of threats that works as a force multiplier. Gangs are going global. They are forging alliances with criminal organizations in other countries. While difficult to say with certainty, it is believed that Solntsevakaya Bratva, the Russian mafia, is the largest criminal syndicate in the world. Yamaguchi Gumi, which has existed for hundreds of years and is known in Japan as *yakuza*, ranks second. Two Italian branches of the mafia, Camorra and N’drangheta, rank third and fourth by size for transnational organized crime organizations, and the Mexico-based Sinaloa cartel rounds out the top five [Genovese, 2016].

Transnational criminal groups include politicians, government officials, and executives who are nothing more than a new breed of sophisticated gangsters, mobsters, thugs, dope dealers, and terrorists who now seek to obtain global power, influence, and monetary and/or commercial gain by illegal means - rather than regional control of territory while protecting their activities through a transnational organizational structure and the exploitation of transnational commerce. The organization comprises countless international executives from varying backgrounds [Sullivant, 2016]. Transnational organized crime is a cooperative activity between criminal groups in various nations, estimated to be a $2 trillion industry [Lipman, 2013].

Some of their criminal activities focus on:

• Attempts to gain influence in government politics and transnational commerce.

• Buying off corrupt officials. Corruption is any abuse of power for private gain. It includes political wrongdoing, bribery of officials, mispresentation, fraud, procurement manipulation, and wrongful reporting. Bribery, corruption, and other white-collar crimes are not solely legal issues; they can have damaging effects on business organizations. This is why security must be the first line of defence of an organization's image, brand, and reputation.

- forging alliances with corrupt elements of governments to threaten governance;
- influencing governments to exploit these relationships to further their interests;
- penetrating state institutions to exploit differences between countries;
- defrauding millions each year through various stock and financial frauds;
- manipulating and monopolizing financial markets, institutions, and industries;
- crime–terror–insurgency nexus [Miloshevska, 2016]. During last two decades criminal and terrorist groups have met a similar evolution regarding their organisational features. They have diversified their models and increased the differences between them in terms of size, or number of members and structures. There has been a transition from the big organisations prevalence with a hierarchical structure and a highly centralised decision-making system (quasi military in some cases) to the combination of the latter with other organisational models and the proliferation of smaller groups, with a more flexible and dynamical functioning and more decentralised structures, including minor networks practically horizontal, some of which have been created spontaneously to undertake just one or few activities but likely to collaborate with other structures from bigger bodies or to be integrated in those.
- intimidation, kidnapping, and assassination;

- disguising the pattern of corruption and violence through legitimate businesses;
- trafficking drugs, humans, body parts, and endangered species;
- trafficking weapons and nuclear materials;
- money laundering and prostitution;
- stealing intellectual property and cyber-crime exploitation;
- using power and influence to further criminal activities;
- isolating themselves from detection, sanction, and prosecution.

In 2000, the United Nations General Assembly adopted the U.N. Convention against Transnational Organized Crime in an effort to call attention to and fight the rise of transnational organized crime. While the document did not formally define transnational organized crime, it recognized that, in general, organized crime consisted of the following:

1) A group of three or more persons who intentionally associate, for

2) A period of time, who

3) act in concert with the aim of committing at least one crime punishable by at least four years' incarceration, in order to

4) Obtain financial or other material benefit [United Nations Convention, 2000].

This loose definition implies that transnational organized crime encompasses virtually all serious profit-motivated criminal activities that could have international implications.

But the lack of the consent regarding what transnational organized crime represents does not prevent researchers from reaching an agreement regarding some features of the phenomenon, considered intrinsic to its transnational character:

A. perpetrators - they are persons or organized groups crossing national borders (physically or virtually - by using advanced technologies in informatics and communications) while developing their activities;

B. the object of the organized crime - is represented by: "illicit goods (manufactured or from the services field); licit goods stealth or those that make the object of smuggling outside the country; the licit goods purchased from a country by violating the restrictions regarding their export; the licit goods imported from a country by violating restrictions regarding import or international embargo";

C. the subject of the organized crime - consists of foreigners engaging in illegal acts on the territory of other state;

D. the motive of organized crime - consists in gaining profit from illicit activities. The involvement in illicit activities presupposes exposure to risks incurred by national legislation constraints. That does not mean that transnational organized crime organizations avoid high risk states. If the latter offer attractive and lucrative markets, then they will become targets for transnational organized groups, that will engage in illicit activities, trying to limit or to minimize their risks, but continuing to operate, mainly, from states where the jurisdiction presents diminished risks for them;

E. the digital signals - refer to the sending of the electronic messages aiming at attacking or destroying the informatics systems or robbing the financial institutions.

According to the operational definition emerging from all of the above, transnational organized crime has three distinct features which distinguish it from its early national manifestations:

a) It operates at regional or global level;

b) It has created extended trans-border connections;

c) It has the capacity to challenge national and international authorities [Stoica, 2016].

In its broadest form, serious organized crime refers to a number of illicit activities that are carried out by a group or groups of individuals on a continuing basis. In essence, these are criminal organizations that work together for the duration of one or more criminal activities. Much as in any legitimate organization, criminal organizations often involve a criminal syndicate or a core group of syndicates at the top of the hierarchy. Similarly, further down the ladder, there may be subordinates, specialists, associates, and runners, depending on their experience and skills. In a further similarity to legitimate business environments, criminal networks engage in a wide range of illegal activity across a wide range of sectors.

Activities include:

- Counterfeiting/Intellectual property crime
- Corruption
- Illegal trade
- Theft of commodities and assets
- Kidnap and extortion

- Money laundering [Crump, 2015].

A particular threat posed by the illegal activities of serious organized crime groups is that their actions may go unnoticed for long periods of time, with the attendant potential for catastrophic consequences for businesses. These consequences may be measured in terms of financial loss, reputational damage, or even direct harm to people and property. However, it is important to note that such activity may not be explicitly illegal. Working under the cover of legal operations, money laundering, bribes, and fraud remain at the core of illegal transactions. In addition, such activity may be further connected to—or even fund—other types of serious organized crime, including smuggling of drugs and people, the illegal arms trade, and terrorism, thereby extending the impact of its consequences from the business itself to the development, operations, and even lives of others.

Intellectual property theft and counterfeiting

Counterfeiting presents a very favourable ratio between potential profits and assumed risks compared to other criminal activities such as drug trafficking. Counterfeiting is a complex criminal activity involving economic, social and legal elements. [UNICRI, 2017].

Counterfeiting is basically creating illegal imitations of genuine products with the intention of fraudulently passing them off as genuine. Products that are especially vulnerable are established brands with a relatively high retail value, such as alcohol, cigarettes, electronics, popular food brands, watches, and clothes. Moreover, illegal imitations include Web sites that imitate genuine commercial Web sites for the purpose of fraudulent activity, such as social engineering [Cabric, 2015].

No brand or label has been able to establish complete immunity from intellectual property theft or counterfeiting. This is evident across flea markets and Internet sites alike, and the news continues to report seizures of counterfeit video games, clothing, and pharmaceuticals. Viagra has arguably shown to be one of the most popular on the counterfeit pharmaceutical market due to its high retail price, while Apple has heightened its manufacturing security following an increase of counterfeit iPhones and other merchandise on the black market [Crump, 2015].

Counterfeiting is now ranked amongst the highest income sources for organized criminal activities.

Corruption and Bribery

Bribery is a criminal practice of giving something (favor, money, services, product, etc.) to gain an illegal advantage. Corruption is basically receiving something to facilitate an illegal advantage. Corruption involves the abuse of position and trust. Engaging in corruption and bribery creates an unfair advantage and an unfavorable business environment. Apart from supporting and strengthening organized crime, corruption is one of the primary obstacles to the economic development of a country and is a main risk that could deter potential investors [Cabric, 2015].

Corruption is perhaps most evident in emerging or unstable economies where transparency is limited or absent altogether. A recent example was illustrated by the IKEA corruption case in Russia, which resulted in the dismissal of the company's two executive managers in the country after allegations of bribery. The scandal emerged after it became apparent that the executives paid off Russian insurance and energy companies to retroactively approve all electrical installations at IKEA's facility in St. Petersburg. While these actions were arguably not directly for the executives' financial gain, their actions did cause direct damage to the integrity of the company [Crump, 2015].

Theft of commodities and assets and illegal trade:

Because variables differ from one asset to another, and from one location to another, and from one business interest to another, and from time to time, no one set of security solutions can apply to the protection of all assets [Sullivant, 2016].

The theft of commodities and assets, e.g., theft of metal from building sites or theft of cargo in transit, remains as an active threat faced by a wide range of industries. With wide-reaching and well-established criminal networks, organized groups are able to move commodities nationally and across borders, avoiding detection much in the same way as those operating illegal drugs or the weapons trade, or even in tangential connection with these operations [Crump, 2015].

Theft may occur from one of two sources: those within the organization and outsiders. Theft can occur when there is a conspiracy between an insider and someone on the outside. It can be motivated by economic gain, a desire for retaliation, or as a means of gathering information. Corporate theft is a situational, opportunistic, and seasonal phenomenon [Sullivant, 2016].

Kidnap and extortion

Kidnap and extortion may also be a part of the wider organized criminal tactics in attempts to coerce, blackmail, or threaten corporations and/or employees into meeting demands, whether financial (in the form of ransoms), regulatory (forcing a corporation to work in a certain way), or physical (handing over assets, operational capability, or information). In 2011, the head of a private security and insurance firm, Peter Stenning in Australia, confirmed U.S. intelligence that indicates Colombian terrorists are working to expand extortion activities [Shanahan, 2011]. The presence of high-profile executives of large, wealthy corporations around the globe can attract the attention of criminals.

Money laundering

Money laundering is a necessary process for organisations that accrue illicit benefits and need to use them for legal purposes. Therefore, reasonably large organisations require more or less sophisticated ways of concealing the illegal source of that income; from sending the money to other countries covertly and circumventing the financial system, to more complex ways such as using shell companies or tax haven jurisdictions [Larsen at all, 2017].

Money laundering is one of the key ‘engines of crime’ sustaining global criminal business worth billions of dollars [SOCTA, 2017]. The task of combating it has become more difficult, due to the increasingly global and virtual nature of financial services and the emergence of technology-enabled factors such as crypto currencies and anonymization tools that frustrate the identification of beneficial owners. Controlling much of this mega-illicit activity are global money laundering syndicates, who offer their services at scale to criminal networks, and are highly adept at exploiting gaps in the financial system. These are the challenging conditions within which anti-money laundering (AML) arrangements currently operate that set a very high bar for success in curtailing the international flows of illicit funds [Europol, 2017].

Finally, what is considered one of the largest money-laundering cases of the twentieth century illustrates the wide extent of illicit activities that corporations may face. The Bank of Credit and Commerce International (BCCI) was founded in 1972 by a Pakistani financier and quickly established an operating capability of over 400 locations worldwide. Its rapid growth—ranking as the seventh largest private bank in the world by assets at its peak—attracted suspicion from financial regulators. Although BCCI contended that its growth was fuelled by large deposits from oil-rich states and developing nations, investigations revealed vast amounts of fraud and money-laundering activities that supported the drug trade and corruption. In addition, it has been alleged that the CIA used the bank to fund the Afghan mujahedeen during the war with the Soviet Union in the 1980s. Following substantial reputational and financial damage, the bank shut down in 1991 [Crump, 2015].

BUSINESSES NEED TO ADAPT TO THE SHIFTING THREAT OF ORGANIZED CRIME

Modern era inflicts necessity that the businesses operate not only within national market boundaries, but also to run in international market race. Having this in mind, companies' cooperation relies on exchange of confidential information that on another side requires protection of this communication against competition, suppliers, consumers, hackers, and other attacks, including espionage [Trivan, 2015].

Corporate security identifies and effectively mitigates or manages, at an early stage, any developments that may threaten the resilience and continued survival of an organisation and its most valuable asset – its employees. In its wider context, it also refers to the practice of protecting customers, physical property and information systems.

Importantly, corporate security should not be seen as a standalone function, but be recognised as having the ability to work with and enhance other areas of the business such as corporate governance and regulation, corporate social responsibility and overall safety assurance.

Recently, Europol released its 2017 "Serious and Organised Crime and Threat Assessment – SOCTA" report [EUROPOL, 2017]. It laid out the challenges legitimate businesses face when confronted by illegal entities that mimic their profit-generating behaviour, but for destructive ends.

But that is only the most dramatic way that criminal and terrorist organisations have changed (although sometimes the same organisation gains funds through criminality, and then uses those funds to finance terrorism). In its report, Europol identifies three other new global trends.

First, criminal organisations have gone increasingly global. With the rise of the Internet, crime groups can achieve global reach in record time. This enables them to exploit new illicit trade markets in new countries rapidly, if demand increases. Like the Internet itself, organised crime has become decentralised.

Second, criminal organisations now offer illegal trade as a service. In the same way that a legitimate business has access to many service providers, organised crime groups now have access to highly specialised, global, and nimble service providers. For example, criminal service providers will specialise in providing stolen identities, raw materials, distribution services, freight forwarding or illegal border crossings.

Crime as a service makes disrupting criminal enterprises extremely difficult. If an enforcement action takes out one "service provider", ten others will be instantly available to fulfil that same need.

Finally, better data analysis is key to successfully combating these global, distributed, decentralised, highly adaptive and fragmented organised crime groups. As [Wainwright, 2017] pointed out, additional information or data is not required, but rather a better aggregation, integration and analysis of existing data. This includes the integration and analysis of multiple dispersed existing data sources.

Too often, corporate security strategies are not aligned with corporate business strategies. Aligning security strategies with business strategies can ensure that corporate security programs are in harmony with company priorities and can place the security director and chief executive on the same page. A valid threat estimate profile helps to achieve this goal. A threat estimate profile helps planners and decision makers to:

- define the level and range of natural disaster, weather-related calamity, industrial mishap, criminal activity, or other major or catastrophic event;
- determine the probability and consequences of threat occurrence and understand an adversary's capabilities, operations, tactics, and support mechanisms;
- provide insight into strategic, tactical, and operational planning; countermeasures development; and program implementation;
- determine staffing needs.

The information that makes up the threat profile is never static. The threat profile is a "living document" that requires constant review and updating as the threat environment changes. It should always be used as a backdrop to developing corporate security strategies, planning, and direction. Not having a reliable, useful, and meaningful threat profile makes it difficult to determine what the highest-priority activity should be when planning and coordinating security operations and initiatives. Any analytical effort would certainly be misguided and ineffective, and more than likely mimic a false sense of accomplishment, leading to excessive and counterproductive labour efforts, less-than-satisfactory performance expectations, and wasteful expenditures [Sullivant, 2016].

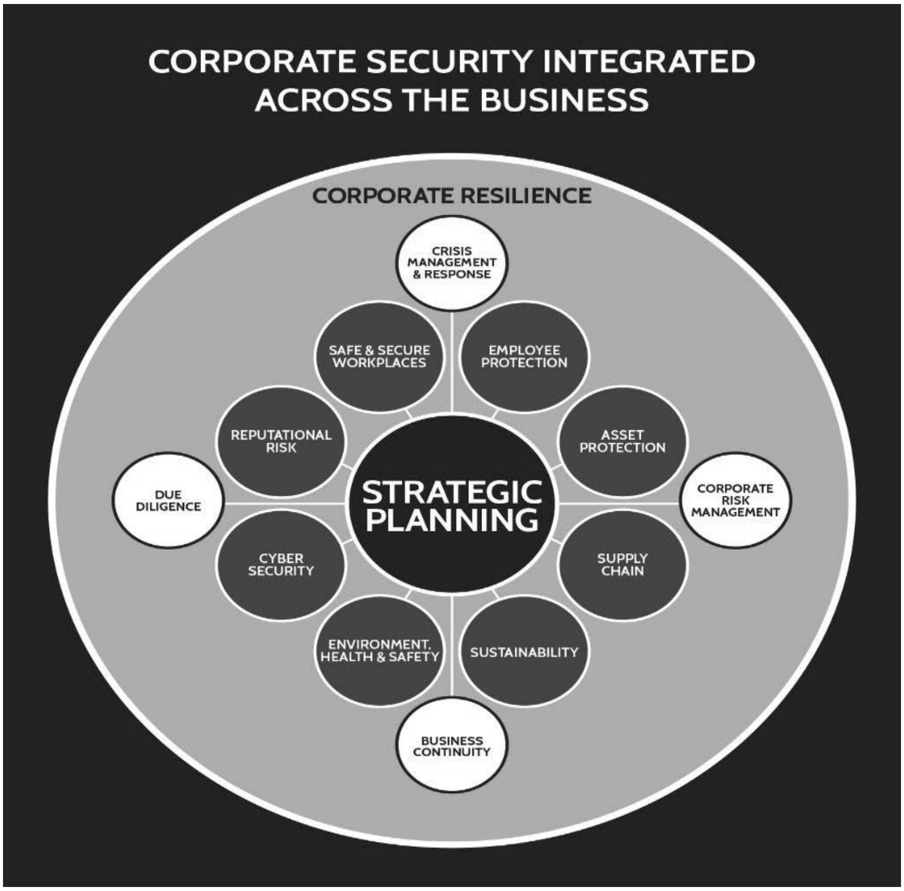


Fig. 1 Corporate security integrates across the business [Haydock, 2017]

Companies need to develop and deploy a comprehensive security strategy across all facets of their business. The framework that we offer below structures such a strategic response according to internal threats, revenue threats and external strategies.

First, internal threats. As a first step, businesses need to focus on shoring up corporate security, cyber security and supply chain security. Every day, organised crime groups attempt to infiltrate the inner workings of companies to gain access to confidential information, employee or customer data, physical locations and distribution systems. Having tight internal controls over physical locations, IT systems, and distribution systems provides the foundation for an effective defence.

Secondly, revenue threats. Businesses must develop a comprehensive brand and supply chain protection strategy, as well as systems and tactics to consistently monitor and defend against illicit trade in their products. Effective brand and supply chain protection will guard businesses against revenue loss, threats to their brand value, and risks to their business investments.

Finally, external strategies. Companies must go on the offense through external strategies that ask law enforcement and government officials to focus on the organised crime and illicit trade impacting their industry. This offensive effort should also include actively engaging with government officials and policy makers to pre-empt or manage unnecessary regulatory burdens [Bergmann, 2017].

A big challenge for organizations is prioritizing, understanding, and addressing threats in a business context.

The insider threat is by far our greatest challenge. Security measures must aim, in part, to minimize the potential of hiring an adversary and to deter individuals from becoming an adversary once they are hired. Such measures must compel the workforce to do the right thing and cause them to take high risks of exposure to do the wrong thing. If an insider chooses to do the wrong thing, security measures must detect such actions early enough and delay the insider long enough so that a response can interrupt the action before it is completed. Current threats are escalating faster than we are able to identify, and they know no geographical boundaries. They can occur at any moment, anywhere—in areas from urban centres to Main Street, targeting small businesses and major corporations [Sullivant, 2016].

In conclusion, the time for businesses to act is now. As the proverb says, “crime never sleeps”. This has never been truer than today. Transnational criminal organisations have evolved into highly organised and adaptive global entities that pose a ubiquitous and pervasive threat for businesses. Businesses need to take action now to shore up their internal defences, build comprehensive brand and supply chain protection programs, and proactively engage government officials, public policy makers and law enforcement officials. By waking up to the threat, they can protect their most valuable assets before becoming a target.

CONCLUSION: A COMPLEX AND MULTIFACETED WORLD

In today’s international marketplace, where many corporations conduct business, corporate assets are blasted by threats to these assets from inside and outside the corporation. The workplace of the modern corporation in today’s “what’s in it for me” environment has changed over the years, as have the societies in which the corporations operate. With the ever growing role and reliance on technology, the threat to corporate assets has never been larger.

With the fast changing global landscape shifting the structure and pace of corporate life, both in the way businesses operate and the environments they work in, security risks are ever more complex.

The range of potential threats facing a company can be overwhelming, and their impact can be high. Even companies that have not traditionally been exposed to more than the most rudimentary of security risks are now exposed to events thousands of miles away, which can disrupt supply chains and highlight dependencies that no one was previously aware of. Threats are networked and are often driven by interrelated issues. Given all of this, and the clear impossibility of forming a total barrier around the business (as may once have been the case), the vital role of intelligence in supporting an agile, dynamic, and efficient security function is obvious.

REFERENCES

1. Bergmann, S., (2017). Businesses need to adapt to the shifting threat of organized crime, *Security Europe*, Brussels, Belgium.

2. Brooks, D.J., (2014). ‘Intrusion Detection Systems in the Protection of Assets.’ In M.Gill (ed.) *Handbook of Security,* 2nd Edition. London: Palgrave Macmillan.

3. Cabric, M., (2015). *Corporate Security Management Challenges, Risks, and Strategies*, Elsevier, UK, USA.

4. Crump, J., (2015). *Corporate Security Intelligence and Strategic Decision Making*, CRC Press, Taylor and Francis Group.

5. Cubbage, C. and D.J. Brooks., (2012). *Corporate Security in the Asia Pacific Region:Crisis, Crime, Fraud and Misconduct.* Boca Raton, FL: Taylor and Francis.

6. Europol Serious and Organised Crime Threat Assessment 2017 (SOCTA 2017), available at: https://www.europol.europa.eu/socta/2017/, access on 20.11.2017.

7. EUROPOL. (2017). From Suspicion to Action-Converting financial intelligence into greater operational impact, Financial Intelligence Group, European Union Agency for Law Enforcement Cooperation (Europol), Luxembourg: Publications Office of the European Union.

8. Hassid O., Masraff A., (2010). La sécurité en entreprise, prévenir et gérer les risques, Paris, Maxima.

9. Haydock, M., (2017). How corporate security can help achieve business growth, EDP the right approaches, available at: http://www.edp-uk.com/news/how-corporate-security-can-help-achieve-business-growth**.**

10. Kovacich, G. L, Halibozek, E. P., (2003). *The Manager's Handbook for Corporate Security*, Butterworth–Heinemann.

11. Larsen H.L., at all (ed), (2017). *Using Open Data to Detect Organized Crime Threats*, Springer International Publishing AG.

12. Lipman, I.A., (2013). Founder and Chairman, Guardsmark, *The Lipman Report*.

13. Michael A. Genovese, M A., (2016)**.** Shape-Shifting Crime in an Age of Globalization, *World Policy Institute*, available at: http://www.worldpolicy.org/blog/2016/06/29/shape-shifting-crime-age-globalization.

14. Miloshevska, T., (2016). Modeli na povrzanost na terorizmot i na transnacionalniot organiziran criminal, Filozofski fakultet, Skopje.

15. Ocqueteau, F., (2011). Heads of Corporate Security in the Era of Global Security, *The social control of violent women*, Vol. VIII.

16. Petersen, K.L. (2013). 'The Corporate Security Professional: A Hybrid Agent Between Corporate and National Security.' *Security Journal* 26/3: 222–235.

17. Roucaute Y., (2010). Une revue scientifique pour penser la sécurité globale, *Cahiers de la Sécurité*, 14, 7-15.

18. Shanahan, L, Mitchell Bingemann, M., (2011). Expert points to Colombian terror tactics, *The Australian.*

19. Stoica, I., (2016). Transnational organized crime, An International Security Perspective, *Journal of Resourse Defense Management*, Vol.7, Issue 2 (13), Ministry of National Defense, Bucharest, Romania.

20. Sullivant, J., (2016). Building a Corporate Culture of Security Strategies for Strengthening Organizational Resiliency, Elsevier Inc., Oxford.

21. Trivan, D., (2015). The Importance and Scope of Business Intelligence Application, Faculty of Business Studies and Law Belgrade, ISBN 005.94:004]:334.72 (497-15).

22. United Nations Convention against Transnational Organized Crime, General Assembly resolution 55/25 of 15 November 2000, available at: https://www.unodc.org/documents/middleeastandnorthafrica/organised-crime/UNITED_NATIONS_CONVENTION_AGAINST_TRANSNATIONAL_ORGANIZED_CRIME_AND_THE_PROTOCOLS_THERETO.pdf

23. United Nations Interregional Crime and Justice Research Institute, (2017). Turin, Italy, available at: http://www.unicri.it/topics/counterfeiting/.

24. Walby, K, Lippert, R.K. (2014). *Corporate Security in the 21st Century Theory and Practice in International Perspective,* Palgrave Macmillan, UK, London.

UDC 005.334:351.759.6

CORPORATE AND SYSTEM COORDINATED INTEGRATION OF SECURITY SERVICES OF STATE AND PRIVATE SECTOR

Prof. dr Ljubo Pejanović[1], Prof. dr Stevan Stojanović[2], Doc. dr Miodrag Komarčević[3]

Increasing of vulnerability to various challenges, risks and threats in contemporary times is characteristic of Europe as a whole, and also of the Republic of Serbia as its integral part. Old and new sources of danger have the potential to inflict harmful consequences on the safety of people, property and the environment, and to endanger the generally accepted values, public order and state interests. In addition to threats that have a regional and interstate dimension, threats also have an economic and environmental dimension, and the most numerous are those related to society itself (social conflicts, illegal migration, various forms of crime, corruption and other deviant behavior). The consequences of these threats can be different in scope, intensity and duration. Prevention and elimination of threats faced by modern societies and countries require adequate organization, corporate co-ordination, coordination and systematic commitment to the integrated approach and joint actions of all relevant stakeholders in the state, private and corporate sectors.

INTRODUCTION

The modern age brought with it new technologies, that is, the achievements in the development of technical means and equipment, which are ap-

[1] *Faculty of Law and Business Studies dr Lazar Vrkatić, Novi Sad.*

[2] *Faculty of Business and Legal Studies, University Union Nikola Tesla, Belgrade.*

[3] *Higher School of Entrepreneurship and Security, Belgrade*

plied in the practice of crime, terrorism and related forms of security threats. In addition to technical achievements, new methods of destructive actions by organized groups are applied with the aim of endangering and threatening overall security. The target of endangering threats are both states and their institutions, as well as corporations and other economic entities, together with the environment and the citizens themselves. In this regard, it is considered that security challenges, risks and threats are interconnected, conditioned, complementary, various in degree terms. They are driven by the understanding of security, as well as the list of protected values and interests (Trivan, 2012).

Modern technology has also contributed to the unprecedented development of mass destruction tools, which represent a permanent security threat in unsatisfactory and disturbed relations in the international community. Modern forms of threat and risk often do not have an adequate response. This is evidenced by the emergence of internal unrest, local wars and regional conflicts that can escalate and extinguish any control. This statement is confirmed by events in the Middle East and North Africa during the last decade (Syria, Iraq, Libya, Tunisia, Egypt, Nigeria, etc.). After the so-called Arab spring this area has been affected by instability, internal armed conflicts and the escalation of Islamic extremism and terrorism (ISIL and its branches, Al Qaeda, Boko Haram and similar groups). The most drastic consequences were in Syria and Iraq, where war conflicts brought heavy devastation, the death of hundreds of thousands of people, and the displacement of the population. In Europe, in 2015 this caused an unprecedented migrant crisis. Although the terrorist structures of ISIL are now defeated militarily, they remain a security threat to the Middle East, and perhaps even more to Western European countries, whose territories have already carried out terrorist actions in recent years. The instability of the international situation is also contributed by the deteriorating relations of Western countries and the Russian Federation, the tensions between the US and North Korea, the internationalization of the conflict in Syria and others.

The Balkan region is also confronted with internal and external threats, as well as with the consequences of the conflicts that took place in the late 20th century (wars in the former Yugoslavia, NATO aggression on the FRY). Along with human losses and material destruction, the consequences of NATO bombing are also related to endangering the health of the population.

The current situation imposes the necessity that state institutions, as well as private and corporate security sector entities, jointly acti on a corporate principle in the prevention and suppression of all forms of threats, hazards and risks. Corporate coordinated actions are of particular importance when it comes to preventing conflicts, terrorist threats, endangering the environment, proliferation of weapons and hazardous substances, and acting in conditions of natural disasters such as floods in the Republic of Serbia in 2014.

Numerous regional corporate initiatives that have been taken so far, related to the improvement of cooperation, agreements and coordination, have made significant progress and have contributed to improving the efficiency of security services and other security actors in the prevention and suppression of terrorist activities, criminal acts and corruption, both in the Balkans and Member States of the European Union.

Different types of national and regional cooperation and coordination of the activities of security entities on the corporate plan aim to create conditions for further improvement of the organization and improvement of security operations. This applies to both the state and the private security sector, as without their corporate coordination, there can be no effective action to prevent and suppress all threatening factors and various forms of security threats (Milošević, 2010).

Conventions, treaties, agreements, protocols, memoranda of understanding and other acts on mutual cooperation regulate issues of common interest to the subjects and institutions of security in order to achieve commonarity in countering security threats. With the same goal, harmonization of the application of unique and related methods of action on the suppression of socially dangerous phenomena that jeopardize security both at the regional, as well as in the European and global regional plan, is being carried out. In contrast, at the national level, the unification of security entities in the prevention and suppression of negative phenomena is regulated by appropriate national strategies, concepts and legal provisions. Further intensifying cooperation and corporate integration of security operations and institutions on a wider scale, certainly contributes to more effective implementation of measures and activities to combat negative phenomena, ie to eliminate or at least reduce the negative consequences of security threats and various destructive activities to an acceptable measure (Pejanović & Stojanović, 2012).

Co-operation, co-ordination and joint action contribute to a co-operative way of performing joint operations and the operation of two or more services in a uniform plan. In this way, the activities of national authorities and services within the state boundaries of a given society, as well as corporate activities with other domestic entities or with foreign security services, are systemically regulated. Corporate activities enable successful actions to prevent and combat negative phenomena and confirm the thesis that the security system functions more efficiently as a single whole (Marković, 2007). In this way, they provide corporate, ie, joint management, and coordinated implementation of measures, actions and activities on a single plan, in order to achieve a common goal. Bearing this in mind, the joint action on countering threats, and thus achieving a higher level of security of society and more efficient protection of its values, shows its full justification. Among many forms of endangering the safety of people and property in times of crisis, there are also almost daily threats, whose activities endanger lives of many people, their health and the overall values that society and citizens have at their disposal (Pejanović & Rakić, 2012). All this is conditioned on the necessity of corporate mergers and co-operation in the field of protection, herefore ensuring security.

THEORETICAL AND METHODOLOGICAL APPROACH TO THE STUDY OF CORPORATE SECURITY

Nowadays, is characterized by the movement and redefinition of traditional perceptions of the paradigm, ie the general perception of the possibilities, needs and modalities of preservation and protection of security at various levels, from the society as a whole, through corporations and other business entities, to ensuring the personal safety of the individual. This largely differs from the previous period and the traditional understanding of security, in which military and political dimension of security were predominant factors. While the state was a reference object of protection in the previous period, in the new strategic documents of many countries the focus of protection is shifting from the state's protection to human security, that is to individuals, their interest groups, and to the economic, ecological, social, cultural and social spheres. Nevertheless, national security, in such conditions, remains a general framework that dominantly defines the mode, quality and conditions for the protection of the life of contemporary man, as well as the security of overall economic, political, social and other trends and processes (Komarčević, et al 2012).

Due to the contradictory processes and the effects of various and turbulent factors, the modern state, and above all those states that have a key influence and role in creating a global security policy and strategy, are compelled to review and redefine security concepts at the national level and accordingly formalize new security relationships and goals.

The fact is that in the modern world there have happened deep systemic changes, the consequences of which have led the policy makers and strategy makers to adopt different thinking and formulating of concepts, content and terms of security, and thus the concept of national security. In academic circles, there is a consensus that today the greatest threats to the international community arise from aggressive threats to other countries, disturbances and threats to state sovereignty and integrity, civil wars, ethnic and religious conflicts, the expansion of international terrorism and transnational crime, the production and proliferation of weapons of mass destruction, disasters, low living standards, poverty, unemployment, deep social differences, hunger threats in some parts of the world, endangering of the environment and others.

Changes in international relations related to these potential threats have also changed security mechanisms that are establishing and developing system solutions, coordination models between competent institutions, and responses to security threats. As far as these changes are concerned, military, security, police, intelligence, judicial, diplomatic and other relevant institutions have been included in them, with the aim of their more efficient action on both the internal and external plan. However, the new conditions imposed the need to find and search for new instruments and mechanisms of operation and significantly changed the framework of challenges and threats to security. On the one hand, it refers to the introduction of new security standards, methods of work and procedures, and to the innovations of planning documents, and, on the other hand, to more actively involve non-state entities in integrated corporate protection measures. Such an approach effectively protects the core values and eliminates security threats to national interests, public order, corporations and citizens.

When a state, society and corporations establish adequate corporate protection measures and when these measures are successfully implemented, basic preconditions for the preservation and defense of social values are created. Bearing all this in mind, there is also the question of adequately defining the security itself and the factors that influence the state of its realization. In this sense, security could mean theoretical research, proofing, prevention and suppression of threats, using integrated protection subjects for the purpose of securing or ensuring the safety of citizens, social order, integrity, sovereignty and material values of a particular society (Pejanović, 2016).

In order to achieve a more complete and more qualitative definition of security, it is necessary to get answers to the questions - what is security, whose security, and whether security is a necessity, ie we should consider safety as a state, security as a function, security as an organization and security as a system .

The answer to the question of what safety is is always linked to reducing threats or eliminating them. In this regard, security is a condition in which there are no threats or those threats are eliminated, which ensures a safe state. Regarding the issue whose security, security is, as a rule, regarded as an appropriate state. Security implies the safety of a society in a healthy environment, and it confirms that security is needed for society, man and its values. By analyzing security as a state with its function or contribution and control over endangering forms of threats and risks, people's safety and the protection of all their values are achieved. Security as an organization is a protected and planned goal that protects the overall social values from various internal and external threats and risks (Komarčević, et al., 2012). However, the idea of achieving security could not be implemented without the established security system that is determined and harmonized by the state and corporations in order to establish the necessary security and protection functions. Consequently, security as a system is precisely a security system that implies an organized institution of a state that carries out preventive and protective activities in order to achieve and maintain the safety of society.

Security in a broader sense is comprehensive and indivisible. As such, it requires the finding of answers that are crucial in understanding the security itself. The question of security is what is the condition, first of all, of the term whose security? When it is recognized who is and for whom the security is intended, it is possible to offer an answer regarding the absence or elimination of threats, while observing this through various values. The second question is security from whom and it is necessary to respond with a flexible and realistic solution. The answer to this question is related to the sources of threats, that is, numerous actors and different threats. If security issues are being raised, it also applies to different security entities in order to achieve the required level of security (Pejanović, 2016).

We should keep in mind that each question raised involves appropriate specific answers and solutions to overcome the problem, which is conditioned on the available security forces on the micro and macro plan, that is, the values that the said forces should protect. When providing a more detailed response to the protection forces, it should be noted that protection is also conditioned on the means that security forces that are engaged in achieving security have at their disposal.

When it comes to international relations, standards and corporate activities on the international, regional and national level, we strive to standardize, harmonize, function and apply viable security. However, the period after the Cold War imposed a new definition of security in the international community. In that sense, some theoreticans including Barry Bazan, a representative of the Copenhagen School of Security, point out that security has three levels (individual, state / national and international security), including several important areas of human activity, primarily military, political, economic, social and ecological environment.

The areas of human activity relevant to national security include the following: the military area includes the offensive and defensive capacity of the state; political area means the state's concern for the organization of its stability, the system of government and ideology that is legitimized; economic area includes the possibility of access to natural resources, market and finance, thus ensuring the necessary level of living standard; the social area determines the existing conditions and the evolution of traditions, culture, language, national identity and customs, while the field of ecology includes the concern for the protection of the biosphere as an essential resource dependent on all human endeavors (Buzan, 1991).

The aforementioned security discourse has become dominant over the past decade, suppressing traditional opinions and discourses in the academic community and the wider professional public. The extent to which the discursive context has arisen in theory, in the media, and in everyday communication is illustrated by examples of the use of terms such as "discursive practice" and "discursive formations" in the discussion of security issues. However, under the term discursive formation, the most commonly understood is the set of accumulated knowledge and experience in the domain of security that can be institutionalized or formalized through appropriate institutionalized forms.

In this regard, it should be noted that discursive practice is in fact the use or application of the existing security discourse and behavior of all relevant security subjects. Security entities in this regard are: political, military, police, intelligence, non-governmental organizations, as well as all security entities in the state and private sectors. However, in the corporate sense, besides the mentioned institutions, civil society, business entities and individuals also have security tasks (Pejanović, 2014). Thus, gradually, in the very foundations of the science of security and its differentiated scientific disciplines, they incorporate existing discursive security contexts that completely change not only the matrix, but also the patterns of understanding and the practice of security. Accordingly, these discourses represent tactical elements or parts of the security and social security strategy, generally accepted social values and values of individuals

The modern concept of human security represents a reference object for the protection of the individual and his social and interest groups. At the same time, human values, which are a reference form of protection, are expanding, moving the focus from political and military to economic, ecological, social, cultural, information and other dimensions of security (Savić & Stajić, 2006). Also, there is a focus on different methods, instruments, mechanisms and tools in preventing and eliminating contemporary security challenges, threats and risks, with a significant expansion of security and protection discourse beyond traditional categories. However, this concept also faces serious criticism of its value, suitability and usability.

On the one hand, in the theory and practice of security, it is evident that efforts are being made to incorporate the concept of human security into modern security agendas. However, attempts at an unreasonable and unprincipled imposition of only one solution or one option, where alternative solutions are not considered, can lead to rapid modification of discourse. In this regard, it should be borne in mind that even the countries that first accepted the concept of human security and incorporated it into their security strategies and policies did not give up their national security systems. Countries that have not done this have almost no chance to access these solutions, since they can not plan or implement their strategic methods in such conditions.

Critics of this approach to security studies feel that the concept of human security has flaws and deficiencies and that it is too stretched. They also believe that this concept is insufficiently formulated and developed, which is particularly important for transitional and post-conflict countries, which would be forced to introduce a new concept of security in the event of abandoning the classical concept of national security. The consequences of abandoning the classical concept of national security, with the introduction of a new, incompletely developed concept, would mean that they enter the security dependency situation, that is, the position in which their own security capabilities would not be able to efficiently secure the safety of society and citizens (Pejanović, 2014).

SYSTEM AND SECURITY SOLUTIONS OF CORPORATE INTEGRATIONS

The concept of corporate-system solutions is based on strategic and conceptual, as well as planned and agreed rules and methods of joint action. Joint operation means the synchronized activities of two or more services from a single system or the combined organization of activities from two related or different subsystems, based on the principle of permanent or temporary association. Generally speaking, the system is a sum of principles that serve as the foundation of a science or as a form of political and social organization or as a sum of ideas, functions, materials, people and groups associated with a particular concept, which represent a complete, relatively independent whole of the system (Political Encyclopedia, 1975).

In this context, the adopted scheduling of the system parts is related to the prescribed principles of work and operation of the security services that are organized into a corporate-unique security system of each state including the Republic of Serbia. Each of them as a subsystem is contained in the system as a single entity that unites and integrates them. Each part of the security system acts according to its legally regulated rules, methods and solutions. However, all groupings within the system are referred to connectivity, association and joint action, at least in certain significant actions that are of interest to a comprehensive or unique security system (Komarčević, et al 2012).

The corporate security system in scientific sense has been derived from a special sociological discipline and is based on scientific bases and legal solutions that must be fully and completely respected. System solutions in this area derive from a set of different, related and similar methods of operation, to which all security operators resort in their professional activities. These planned activities are based on the ultimate goal of achieving planned and entrusted tasks. In this case, each individual subsystem implies a special form of social organization on a corporate plan within a single system, the goal of which is to eliminate all possible or existing forms of security risks and threats. Security risks are considered potential threats to citizens, social and private values, the security system and the social order of every democratic society. Certain security threats can pose a threat to both the regional level and even the international community as a whole (Pejanović & Stojanović, 2012).

The scientific and theoretical concept of the security system at the national level implies the study of security sciences as a whole, or individual scientific disciplines from the field, including security basics, security systems, national security, corporate security, civil security, military security, private security, security management and others. Arranged on the basis of theoretical concepts and legal solutions, the national security services, authorities and institutions make a set of equal institutions integrated into one whole - a security system based on corporate principles (Savić & Stajić, 2006).

Bearing in mind all of the above, the unique security system includes a set of independent and equal entities that are organized in a coordinated way to prevent and combat any negative phenomena that pose potential risks and threats to the security of people, material values, the environment and the national security system (Pejanović, 2016).

The systemic corporate organization of all security entities in terms of preventing, suppressing and eliminating negative and destructive phenomena that endanger security in general is precisely the condition for achieving the ultimate goal - ensuring personal and property safety of citizens by using common forces in a unified and comprehensive system. In addition to the joint action of the security forces in a unified national system, there are situations in which the association and cooperation of national security services with the security services of other countries at the regional and wider global level are necessary. In this context, as a rule, intergovernmental agreements and memoranda on joint actions, in the first place, are dealt with, at the level of the ministries of the interior (less than the ministries of justice) and the director of national police, in the area of cross-border crime, terrorism and illegal migration. Such interstate or multilateral agreements are the basis for undertaking actions in the territory of two or more states with the aim of eliminating transnational threats of security. [4] In this regard, it should be borne in mind that the systemic integration of services, businesses and activities across a corporate system implies corporate governance and action in response to various security threats and risks at the national, regional and international levels.

The historical context of corporate security integrations in the Republic of Serbia

By analyzing documents and practices from the period of the former SFRY, it would be possible to draw a wrong conclusion that at that time there was no representation of corporate governance and the functioning of defense and security services on the national and international level, but rather that this was the achievement of the newer era and the implemented democratic reforms. However, corporate security integrations existed in the previous system. Namely, in the former Yugoslavia, at the federal level, there were ministries of foreign affairs, security services and a unit of the armed forces and police services in the Federal Ministry of the Interior. These services and forces were essentially the basis of corporate action within the common state, but did not have jurisdiction over the relevant services and forces of the Republic. As for the joint actions and participation of the then SFRY defense and security forces within the international forces, this was not legally allowed due to the country's neutral foreign policy.

Protection of independence, constitutional order, defense system and internal security have always been at the forefront, which is why defense and security doctrine and strategy have been based on defense against all ex-

[4] One of the examples of these agreements is the agreement between the Republic of Serbia and the Republic of Croatia on the mutual extradition of the citizens of the two countries who have committed crimes for hiding across the borders of these countries. This agreement also implies joint actions to prevent and combat organized crime in those two states.

ternal and internal threats and hazards. The threats, hazards and risks that emerged were suppressed by the federal and republic security forces, in some cases independently, and sometimes in joint or corporate actions (Pejanović, 2014). The most famous examples of corporate actions of the security forces of the SFRY were the joint action of the federal armed and police forces and the federal units of the Territorial Defense of Bosnia and Herzegovina on the destruction and liquidation of the Ustasha terror group in the Raduša mountain area in 1972, and the suppression of the separatist rebellion or the demolition of demonstrations in Kosovo and Metohija during the 80s and early 90s of the last century by the federal security forces. In this connection, a joint police battalion was formed at one time by the forces of the federal and republican ministries (secretariats) of the interior (Pavlica, 2006).

In the view of all the above mentioned facts, in the former SFRY, the organization of joint activities, that is, the corporate operation of military and security forces was exclusively present within state borders, while international security cooperation did not exist in this sense. Therefore, it is possible to talk about the differences related to the association, integration of forces and the joint operation of the services at the time and the current situation, in which there is a possibility of corporate association or organization.

Democratic changes and reforms in the social order and security system in the Republic of Serbia have brought about great changes in relation to the internal and external security policies, which are fundamentally different from the ones characteristic of the former Yugoslavia. In the last two decades, comparative experiences and knowledge have increasingly been applied, including the acceptance and use of models of other, especially developed countries, according to which the integrations of individual subjects and security operations are useful, and necessary in overcoming the danger of many possible threats and risks. Namely, corporate mergers, communication and joint actions with relevant subjects of neighboring countries reduce risks and threats, primarily those arising from the immediate environment, and then those related to the wider international community. In this sense, there are various forms of corporate co-operation and international integrations,, starting with the NATO Partnership for Peace program, including participation in various peace missions and operations.

CORPORATE-COORDINATED ACTIONS IN THE FIGHT AGAINST POSSIBLE THREATS

In security theory and practice, there are essential differences in the conceptual definition of corporate security within the national state and its environment, and therefore the view of its content. In this sense, the differences also relate to the realization of security within the borders of the national state, and to security beyond its borders. In this regard, if they observe possible forms of threat to the security of the state, they can not be the same and of the same intensity within the borders and beyond national borders. Within the country's borders, security can be jeopardized by parts of the dissatisfied population through various ways of expressing dissatisfaction - strikes, demonstrations, rebellions, attempts at the revolution, provoking conflicts with security forces and even terrorist actions. In addition, the security of the state is endangered by organized, violent, economic and ecological crime, corruption and other forms of deviant behavior and action (Skakavac & Simić 2008). It is also possible to establish agents of foreign intelligence services, or to create a fifth column in situations of external aggression on a given state.

External forms of security threats and risks are diverse and numerous in relation to the internal ones. They are primarily present in:

a) non-military threats, including terrorism, transnational organized crime, military threats and pressures, economic sanctions, boycotts and blockades, intelligence-subversive activities, propaganda campaigns, incitement, and aiding internal rebellions and the like (Skakavac & Simić, 2008);

b) military threats, including armed aggression, military interventions and limited airborne actions, sea or land combat operations, military support to internal rebel forces (weapons supplies, equipment and financial assistance), the organization of military training camps, organization and assistance to terrorist activities and other.

Consequently, the concept of corporate integration of security forces and affairs implies corporate-integrated organization, association and joint action of all security entities within state borders to prevent and combat threats and risks, with corporate management of forces and jobs. In addition, corporate integrations also include cooperation, coordination and provision of security assistance beyond the borders of the state, and according to each official invitation from the assisted country, with the aim of unified action on the suppression and elimination of threats (Pejanović & Rakić, 2012).

Strategic approaches to modern security system reforms are based on realistic assessments, assumptions, and expectations, to achieve the improvement of the quality of the operation of the security sector by integrating services and jobs. Corporate merging of services and jobs on the national level facilitates better coordination, cooperation and operation of entities, systems and activities, on the international level as well. In this regard, it should be noted that modern challenges, risks and threats to security imply the need to redefine missions and tasks in the defense and security system of each state, including the Republic of Serbia. The violent breakup of the former SFRY led to a situation in which the Republic of Serbia faced various challenges and numerous potential sources and forms of threats, hazards and risks (riots, demostration, terrorism, organized crime, external aggression, natural disasters, illegal migrations, etc.). All of the above mentioned is conditioned on the reform processes, both in the domain of the political system and socio-economic order, as well as in the area of the state and private security sectors. In addition, various regional initiatives related to the improvement of cooperation and the establishment of certain types of coordination of the competent services and bodies in the security sector have been initiated, which have led to positive developments in improving the efficiency of the security services both in terms of prevention and the suppression of various security threats , especially those related to terrorism, criminal activities and corruption (Pejanović & Stojanović, 2012).

All the challenges, threats and risks bring with it certain consequences, which requires appropriate state responses. Timely and effective responses are related to reforms, harmonization and improvement of the current situation, in order to achieve better results than those achieved before transformations and reforms. Timely assessment of challenges, risks and threats to the safety of society has the basic purpose of providing adequate preventive action in taking appropriate measures, actions and activities. It also enables the defense and security system to reach the level of competence for an adequate state or private response to any expected and endangering threats. In this regard, the Republic of Serbia has embarked on democratic reforms of both social order and the defense and security system, as well as more adequate cooperation among the countries in the region and the wider international community. Cooperation and coordination of the defense and security forces of Serbia with the forces of other states and entities of the international community is co-ordinated by numerous signed treaties and agreements related to joint activities and activities on the prevention and suppression of organized crime, corruption, terrorism and other security threats.

Strategic cooperation and coordination between states as well as organs within a state, involves military and non-military cooperation. Under the non-military cooperation and joint actions of the security organs of the Republic of Serbia with the security institutions of other states, there are primarily the prevention and suppression of terrorism, as a modern phenomenon that threatens the entire international community, as well as organized crime. In this sense, similar cooperation is needed on the military level, which was done by sending peacekeeping military missions to war crises affected areas of other countries and regions. In recent years, co-operation and coordination in joint actions on the prevention and suppression of organized crime has been further strengthened, because those crimes pose a threat to the systems of all countries in the region as well as the international community.

Regarding the unification of jobs and activities and the participation of members of the armed forces of the Republic of Serbia in international peacekeeping forces, this issue is regulated by international and interstate agreements. The aforementioned agreements stipulate that members of the armed forces of Serbia may participate in the peacekeeping forces in vulnerable areas exclusively as peacekeepers.

In the past period, the Republic of Serbia has also initiated joint actions to help protect and save people and material assets from natural disasters and accidents by sending assistance in the form of trained people and material resources to many endangered countries in the world. One of the newer examples was provided assistance in the earthquake in Haiti. The agreements signed include the sending of peacekeepers to other countries, including Congo, Ivory Coast, Lebanon, Cyprus, Afghanistan and others.

The integration of jobs and activities of two or more services or security entities on a corporate principle can be implemented on a national and international level. If integration implies the merging of several parts into one group, it is about integrating different and related services into one whole or entity - in this case i is a national security system, which implies corporate mergers. In accordance with the provisions of the Constitution of the Republic of Serbia, the security services constitute one whole through the security system of the Republic of Serbia. Within this system, all defense, security and protection services are organized, such as: armed forces, security agencies, intelligence agencies, public security, civil security, corporate security, private security, civil protection and other security and safety entities. All of these entities are equal and independent in achieving their planned tasks. They are at the same time referred to coordination and cooperation in order to more effectively solve tasks in achieving system security. All of these entities are in this case in one system and thus constitute integration into one whole, through which they fulfill their roles, obligations, goals and tasks. However, in addition to the integration of services and their tasks through the unique national system of a state, it is possible to integrate and link services, entities and businesses beyond the borders of the national system (Milošević &Dostić, 2009).

The integration of individual entities of the national armed forces of two or more states implies integration into international forces, such as those in Bosnia and Herzegovina, Kosovo and Metohia, Afghanistan, Iraq and other war-affected areas. The integration of national armed forces into one organization or system also provides for the NATO alliance, which includes the integrated parts of the national armed forces of 19 states.

In addition to the integration of the armed forces, there is also the possibility of establishing an organized and integrated system consisting of individual members or parts of national police forces, which is the case with INTERPOL, EUROPOL and other organizations of that kind in the contemporary international community (Lučić, 2004). In addition to integrated forces with members of armed units and police services, solutions are also available regarding the integration of joint actions in the prevention and suppression of terrorism, grave crimes and organized crime. The integration of activities involves the delivery of criminals of one state to another country whose citizens have committed a crime in that country. With this problem, the former republics of the SFRY met upon the end of civil wars. In this connection, at the request of the international community, ie the Hague Tribunal , the citizens of Croatia, Bosnia and Herzegovina, Serbia, Kosovo and Montenegro, who were charged with genocide and war crimes, were delivered.

Integrated security, judiciary and similar jobs in the present day are being realized in the territory of Kosovo and Metohija. Since 1999, members of the international armed forces, the police, and the judicial authorities have been deployed in this area, whose tasks concern the joint realization of security in that territory, due to the impossibility of the presence of security entities of the Republic of Serbia under Resolution 1244 adopted by the United Nations Security Council (Pavlica, 2006).

CORPORATE-INTEGRATIVE ACTIVITIES WITHIN A STATE - AN EXAMPLE OF AIR TRAFFIC

One of the forms of corporate association of professional services and jobs on national and international level is the integrated development and control of civil aviation traffic. This practice and experience can be applied by one or more states, including corporate aviation management, with the aim of achieving greater safety and security of this type of traffic. Otherwise, air traffic, or air transport of people and goods, can be developed within a single state using only its airspace, as well as using airspace, facilities and resources of other countries.

Integrative organization of services, or entities and businesses in companies and corporations, is most often organized within state borders, with the aim of achieving an adequate level of air traffic safety. In some cases, key corporate systems, such as airports, as a rule, are protected by the state entities in cooperation with other services, since this is a territory of special state interest (Rakić & Ostojić, 2003).

The military as a national authority has the role of protecting the national airspace from unplanned intruder aircrafts, such as unannounced or abducted aircrafts, which includes their return or detention to the destination. Police as a state entity undertake preventive and repressive measures and activities in the protection of air traffic from all forms of threat. Customs authorities and offices at airports also take appropriate measures, actions and activities to prevent the smuggling of weapons and hazardous materials in order to protect people and material assets from being threatened. Company and private security and security services take preventive measures and activities in preventing all forms of threats at airport facilities and aircraft, as well as in the interior of facilities.

INTERPOL is a security entity that carries out activities at the same time both nationally and internationally. This international police organization operates in all internationally recognized states, organized and controlled by a single center - the General Secretariat. The role of this subject is the prevention and suppression of unlawful acts in the entire area of the international community. The General Secretariat of INTERPOL consists of five sub-directories - for Africa, America, Asia and the South Pacific, Europe, the Middle East and North Africa, and the Subregional Coordination Office. The essence of the organization of this bureau is to realize the practical needs of the prosecution authorities of each region, since they differ in the issues and each region is specific in its own way. All regional centers are organized in a unified system, which is a precondition for INTERPOL to be a successful organization in the corporate system. A similar organizational structure within the European Union is EUROPOL, whose role is related to intelligence police activity on the prevention and suppression of terrorism, illegal trafficking in narcotics and transnational organized crime in the European Union. All this confirms the justification of corporate organization os associations of security, which allows for more efficient operation and creates conditions for achieving the security goals that are aimed at (Djukanović & Nikolić, 2008).

CONCLUSION

In complex state structures and supranational communities such as the United States, the former Soviet Union (USSR), the European Union (EU), the former Socialist Federal Republic of Yugoslavia, and others, it has been possible to link certain systems that have their specificities into a unique and functional system . The corporate form of organization and functioning served as the basis for organizing and forming common defense and security functions within current and former military alliances, such as the NATO Pact and the former Warsaw Alliance. To this end, joint functions of national police services are organized in specialized international organizations such as INTERPOL and EUROPOL.

Since the NATO Pact was established as a unified system for the collective defense of member states, in practice it turned out that the United States has a key influence in that military alliance, while European members are in a subordinate role. A certain form of its own defense and security forces (ESDP) has been established by the European Union, again in close cooperation with the United States.

The above examples of organizing, integrating and functioning of defense and security forces from the composition of several countries in practice have demonstrated efficiency, power and impact strength. However, their role has often emerged from the framework of defensive functions, as evidenced during the conflicts in the former SFRY territory, as well as in military interventions in Afghanistan, Iraq, Libya and other areas. In this sense, certain alliances in addition to defensive and security functions represent a threat to non-member states, especially smaller and weaker, and may be a source of jeopardizing their sovereignty.

There is also a practice where several countries organize joint forces in order to improve defense and security power, from the aspect of improved numbers, training, equipment and efficiency of operations, especially on the preventive plan. The most important part of this is deterring from threats, which aims at preventive protection from endangering dangers, without offensive and aggressive ambitions. Such a strategy represents the most effective security protection without any special investment, risk and consequence. These are examples that are relevant for the Republic of Serbia (Pejanović, 2014).

The above-mentioned supranational forms of organization indicate the need for the formation of strengthened forces at the national level. By integrating smaller services into multiple levels of organization, it allows countries to more effectively realize defense and security functions in relation to dispersed and poorly integrated structures that do not have sufficient capacity to protect security from various threats. In this regard, the possibility of corporate integration of security services into a functionally unique system could be considered in the Republic of Serbia, in order to avoid mutual rivalry, non-compliant views on security priorities, and different approaches to training, equipping, education and acting in extraordinary circumstances.

The security services in the Republic of Serbia, including the Ministry of the Interior and the armed forces, do not have the security power to the extent necessary for the most difficult security challenges. This concerns the number and structure of their members, as well as the equipment and resources that they have at their disposal, which makes them individually not an effective force that could successfully confront the most serious security threats of the present.

Past theoretical and practical experiences and indicators from the practice support the thesis that private security and safety services need to be reorganized into one corporate subsystem in a unique national security system. This form of organization would create the conditions for more efficient supervision of the legality of the activities of those entities

Corporate-system solutions, planning, negotiation and harmonization of joint actions and the application of experienced methods of operation create the conditions for more efficient integration of services and security operations. All this leads to a unique goal - elimination or reduction to the smallest possible extent of various negative phenomena that endanger security. Namely, every threat to security imposes risks with hardly perceptible consequences, from the local level, through the state, to the global international community (Pejanović & Stojanović, 2012).

REFERENCES

1. Đukanović, D. & Nikolić, G. (2008). Saradnja država jugoistočne Evrope u oblasti unutrašnjih poslova i pravosuđa, Nauka, bezbednost policija, Vol. XIII, br. 1, Kriminalističko-policijska akademija Beograd.

2. Komarčević, M., Pejanović, Lj. & Živanović, C. (2012). Korporativna bezbednost, Visoka strukovna škola za preduzetništvo, Beograd.

3. Lučić, S. (2004). Razvoj zajedničke spoljne i bezbednosne politike u Evropskoj uniji, Bezbednost,Vol. 46, br. 2, MUP Republike Srbije, Beograd, str. 177-190.

4. Marinković, N. (2007). Stvaranje odbrambeno-vojne strukture u Evropskoj uniji - prepreke i mogućnosti, Nauka bezbednost, policija, Vol. XII, No. 1, Kriminalističko-policijska akademija, Beograd, str. 111-125.

5. Marković, S. (2007). Osnovi korporativne i industrijske bezbednosti, Fakultet za pravne i poslovne studije, dr Lazar Vrkatić, Novi Sad.

6. Milošević, M. & Dostić, S. (2009). Saradnja graničnih policija zemalja Evropske unije -primer SR Nemačke i Poljske, Strani pravni život, br. 2/2009, Institut za uporedno pravo, Beorad, str. 253-269.

7. Milošević, M. (2010). Pojam i sadržaj korporativne bezbednosti, Naučni skup „Dani bezbjednosti (zbornik radova), Fakultet za bezbjednost i zaštitu, Banja Luka, str. 59-60.

8. Pavlica, B. (2006). Saradnja državne zajednice Srbijja i Crna Gora i Repulike Makedonije u borbi protiv albanskog ekstremizma, Bezbednost, Vol. 48, br. 1, MUP Republike Srbije, Beograd, str. 132-148.

9. Pejanović, Lj. (2016). Osnovi bezbednosti, Fakultet za pravne i poslovne studije dr Lazar Vrkatić, Novi Sad.

10. Pejanović, Lj. (2014). Perspektiva korporacijske bezbednosti kao konvencionalnog subjekta bezbednosti u sprečavanju destruktivnih akata u korporacijama, Sedmi medjunarodni skup "Dani bezbjednosti", Fakultet za bezbjednost i zaštitu, Banja Luka, str. 103-113.

11. Pejanović, Lj. & Rakić, M. (2012). Neki oblici ugrožavanja čoveka u kriznim vremenima, Međunarodni naučni skup „Reforma na bezbednosniot sektor vo Republika Makedonija", Evropski univerzitet u Skoplju, Skoplje.

12. Pejanović, Lj. & Stojanović, S. (2012). Sistemski koordinirano suzbijanje pretnji, Međunarodni naučni skup „Reforma na bezbednosniot sektor vo Republika Makedonija", Evropski univerzitet u Skoplju, Skoplje.

13. Politička enciklopedija (1975). Savremena administracija, Beograd.

14. Rakić, M. & Ostojić, M. (2003). Upravljanje vazdušnim prostorom kao faktor bezbednosti, Beli Anđeo, Šabac.

15. Savić, A. & Stajić, Lj. (2006). Osnovi civilne bezbednosti, Fakultet za pravne i poslovne studije, Novi Sad.

16. Skakavac, Z. & Simić, T. (2008). Uticaj sredstava masovne komunikacije na kriminalitet maloletnika, Zbornik radova, Visoka škola unutrašnjih poslova, Banja Luka, str. 135-150.

17. Trivan, D. (2012). Korporativna bezbednost, Dosije studio, Beograd.

UDC 343.533::004

THE ROLE OF CORPORATE CYBER-SECURITY

Full Professor PhD Aleksandra Stankovska
Faculty of Economies at European University –
Republic of Macedonia, Skopje
Associate Professor PhD Ferdinand Odjakov
Faculty of Detectives and Criminology at European University –
Republic of Macedonia, Skopje

Today the economic health and security of corporation is critically dependent on the internet and its technologies. Corporate secrets, financial records, and official companies' data are all increasingly vulnerable. Cyber criminals can significantly threaten the finances and reputations of corporation. Given the abundance of potential victims and profits, cyber criminals will likely continue to target corporation. Similar to financial and reputational risk, cyber security risk affects a company's bottom line. It can drive up costs and impact revenue. The risks associated with any attack depend on three factors: threats, vulnerabilities and impacts. Cyber-security is in many ways an arms race between attackers and defenders. The management of risk to information systems is considered fundamental to effective cyber-security.

INTRODUCTION

Over the past several years, experts and policymakers have expressed increasing concerns about protecting ICT systems from cyberattacks—deliberate attempts by unauthorized persons to access ICT systems, usually with the goal of theft, disruption, damage, or other unlawful actions. Many experts expect the number and severity of cyberattacks to increase over the next several years.

Cybercrime climbs to 2-nd most reported economic crime affecting 32% of corporate organizations. Vulnerabilities in corporate's infrastructure can compromise both corporate current financial situation and endanger its future. Cyber-attacks are estimated to cost the global economy €400 billion every year.

Corporate security is process that identifies and implements all necessary legal measures to manage security risks in the individual corporation. As such, it represents one of the basic functions of the corporation's operations and for its efficient functioning strictly implemented in close collaboration with all other key functions within the corporation. Corporations must take steps to address many types of risk—financial, operational, reputational, and others. But as business becomes ever more reliant on technology, addressing catastrophic risk—losing all data, production systems, or intellectual property—must also be on every executive's agenda.

Every corporation has a vested interest in the property it owns, and security measures are implemented to ensure the protection of physical items, corporation -owned ideas and the network its computers use to function. At the most basic level, corporations need to protect the physical property they own. Different industries require different security measures to achieve this objective. Corporations that manufacture food or drug products have tighter security in regard to allowing employees and visitors into restricted areas than a retail outlet. Retail stores have their own issues in regard to security: Loss prevention is an important detail for this particular industry; security personnel need to focus on it.

The ideas employees develop for their employers are considered intellectual property, and organizations typically own the rights to this form of property. Corporate security is concerned with making sure that an organization's ideas are not stolen and taken to a competitor. One way to proactively prevent intellectual property theft is to restrict access to computer files on the company's internal network. Not all employees need access to all files, and documents containing valuable information should be protected.

With the accessibility of information contained on computers connected within a company network, network security is an emerging concern for corporations. Corporations need to not only secure the information from external threats, but they also need to defend against any form of viral attack. Whereas a company's security department is most likely to be concerned with physical damage, this kind of security is handled by an information technology department. Measures to protect a company's network include: limiting employee Internet access, scanning email for viruses and establishing a limited intranet that's not connected externally.

For many years corporate security has been dominated by a 'defensive' approach, focused on protection and loss prevention. Cybersecurity the protection of valuable intellectual property and business information in digital form against theft and misuse—is an increasingly critical management issue (www.mckinsey.com).

The chances of a business or an individual becoming the victim of a cyber-attack have never been greater. But although awareness of cyber threats has never been higher, many businesses continue to fall into dangerous traps as they deal with the complexity of securing a digital enterprise.

When it comes to cyber risk, the mismatch between perception and reality is great. Natural optimism bias combined with a lack of understanding of cyber risk can lead business executives believing that their businesses are secure. While cyber risk may never go away, understanding the reality can help many companies take action to lower this risk.

The reliance placed on information systems, both for the storage and transmission of data, is making data security breaches all the more damaging to corporations. It has never been clearer that corporations need to have data security policies in place and good information governance.

Cybersecurity has never been more essential, for at least four major reasons. First, companies have more digital assets than they did 10 years ago, and these assets are worth more than they were before. They include customers' personal, financial and transaction information; proprietary assets, including source code for products; automated business processes; sensitive communications with suppliers and partners; and other data. The security around these assets varies greatly depending upon the perceived (as opposed to the actual) financial and strategic value to the business, as well as the effectiveness of the security technologies and processes in place (http://www.bain.com).

What's more, organizations are shifting to hybrid cloud architectures as they continue to adopt software, security and other solutions as services

(SaaS, SECaaS and so on). Historically, digital assets were protected within the company's data center, where it was easier to guard the perimeter and manage user access, authorization and authentication from known locations and devices.

Secure Works Counter Threat Unit (CTU) ™ is made up of a team of professionals with backgrounds in private security, military and intelligence communities, and has been publishing threat analyses since 2005. The CTU uses threat visibility across thousands of customer networks to identify emerging threats as well as many other resources including (www.secure-works.com):

1. Attack telemetry from clients;
2. Malware samples;
3. Investigations;
4. Public & private information sources;
5. Website monitoring;
6. Social media;
7. Communication channels used by threat actors;
8. Security community; &
9. Government agencies.

Today, corporate and customer data resides in the organization's own data centers as well as public and private clouds, distributed across remote locations. While hybrid cloud architectures offer significant economic benefits, their adoption requires a more sophisticated approach to cybersecurity, including security management at the level of individual digital assets and integrated monitoring and management capabilities across the hybrid cloud environment.

Potential threat sources and actors include: terrorists, criminals, foreign intelligence services, competitors, hackers, activists, malware developers, employees, and contractors.

METHODOLOGY

To achieve the object of this paper, the corporate security and cybersecurity data has been collected. The primary information is mostly from websites, books, journals, etc.

ANALYSIS AND DISCUSSION

Companies are increasingly becoming growing targets for cyber-attacks. Treasuries are working tirelessly to upgrade their cyber-fraud programs in order to protect their organizations and keep up with the escalating pace of cyber-crime. Not all attacks are about theft or destruction. A more sinister cause is the manipulation of data in place – such that machines can be controlled – or the wrong information reported to human operators without their knowledge.

Cyberattacks are costing global businesses as much as $500 billion per year. The banking and financial sectors have led the way as top targets for cyberattacks in the last five years, with IT and telecom, defense, and the oil and gas sectors following behind. The biggest threats in cybersecurity today are around the large scale proliferation of targeted attacks – from breach and email distribution of socially engineered ransomware to potentially harmful attacks on critical infrastructure like energy networks.

Advanced threat actors such as nation-states, organized cybercriminals and cyber espionage actors represent the greatest information security threat to enterprises today. Many organizations struggle to detect these threats due to their clandestine nature, resource sophistication, and their deliberate "low and slow" approach to efforts. For enterprises, these more sophisticated, organized and persistent threat actors are seen only by the digital traces they leave behind. For these reasons, enterprises need visibility beyond their network borders into advanced threats specifically targeting their organizations and infrastructure. This is known as threat intelligence. (Roger A.Grimes, 2018)

The hacking methodology contains the following progressive steps (Roger A. Grimes, 2017, pp.11):

1. Information Gathering;
2. Penetration;
3. Optional: Guaranteeing Future Easier Access;
4. Internal Reconnaissance;
5. Optional: Movement;
6. Intended Action Execution; &
7. Optional: Covering Tracks.

Having a strong plan to protect corporate organization from cyber-attacks is fundamental. So is a recovery plan to help corporation deal with the aftermath of a potential security breach. These plans can also become leverage for company. Investors think highly of those managers who are prepared to deal with every imaginable scenario that the company might experience (https://heimdalsecurity.com).

As part of their cyber security policy, companies should ((https://heimdalsecurity.com):

- Identify risks related to cyber security;
- Establish cyber security governance;
- Develop policies, procedures and oversight processes;
- Protect company networks and information;
- Identify and address risks associated with remote access to client information and funds transfer requests;
- Define and handle risks associated with vendors and other third parties; &
- Be able to detect unauthorized activity.

What the news does every day is to point out that companies everywhere are vulnerable. This is true irrespective of their sector, size and resources. There are two forces which are pulling in different directions: the attackers, who are getting better at faster at making their threats stick and the companies, which still struggle with the overload in urgent security tasks.

On the other hand, after analyzing the views presented in the cyber strategies of the developed countries, cyber activities can, in principle, be divided into four groups (G.Matic & M. Miljkovic, December 2013, pp.42):

1. Cyber-crime;
2. Cyber terrorism;
3. Cyber espionage; and
4. Cyber warfare.

Cyber threat actors are expanding the uses of computer network exploitation to fulfill an array of objectives, from the economic to the political (www.fireeye.com). In cybercrime, three distinct classes of threat actor have been identified (www.globalservices.bt.com):

- The Cyber Criminal – organized crime (corporates are high profile target);

- The Cyber Terrorist – non state actor (corporates are target, but trading platforms and clearing houses are high profile targets); &
- The Hostile State Actor – cyber warfare (corporates are target, but trading platforms and clearing houses are high profile targets).

In security parlance a threat agent is an attack source combining motivation and capability. In general, threat agents can be categorized from benign to critical.

Cyber threats actors could be financially or socially motivated hackers, disgruntled employees, organized criminal gangs, competitors or state actors. Some of these actors are well trained and will persist a campaign to achieve their goal of data theft or damage over weeks to months. A well-organized cyber threat management is needed to detect and stop these threats.

Threat actors are constantly inventing new tools and techniques to enable them to get to the information they want and are getting better at identifying gaps and unknown vulnerabilities in an corporate's security (www.ey.com):

- State-sponsored espionage (the actor or group is employed by the government of a nation-state), also referred to as Advanced Persistent Threat (APT), is typically very quiet and practices operational security. The main objective is to support a nation state's economic, political or military objectives;
- Organized crime is groups of criminals that intend to engage in illegal activity, most commonly for monetary profit. Attacks are designed to either extort money from the target, or the actors are funded to carry out an attack (www.surfwatchlabs.com);
- Organized cybercrime activity is primarily driven by financial gain, but will also target data assets that can be traded to others. Organized criminals increasingly purchase components they need to commit crime through online marketplaces. Criminals are becoming increasingly more sophisticated and often use blended attacks (technical and social engineering); &
- Hacktivism actor – an actor that performs attacks in order to draw attention to a cause (such as free speech or human rights), or hinder the support of a cause. If the cause is political, and/or designed to inflict terror, they are instead considered a Cyber terrorist.

Hacktivism actors can be quite loud in comparison to other threat actors, often using social media to discuss operations and to recruit members to attack a target. They are focused on damaging reputations, causing disruptions and making derogatory statements about organizations they do not agree with. Hacktivists have captured media attention with campaigns coordinated through social media. Favored criminal techniques include SQL injection and DoS.

Eliminating threats is impossible, so protecting against them without disrupting business innovation and growth is a top management issue.

Today's cybersecurity threats include indiscriminate and broad-based attacks designed to exploit the interconnectedness of the Internet. Increasingly, they also involve targeted attacks, the purpose of which is to steal, manipulate, destroy or deny access to sensitive data, or to disrupt computing systems. These threats are exacerbated by the interconnected and interdependent architecture of today's computing environment. Theoretically, security deficiencies in one area may provide opportunities for exploitations elsewhere.

Cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets. Organization and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment.

Figure 1

Common threat agent categories and their typical vectors

THREAT LEVEL	THREAT AGENT	THREAT VECTOR
CRITICAL	Nation state	Espionage, theft, sabotage, product alteration
	Competitor	Espionage, theft, product alteration
	Organized crime	Espionage, fraud, theft
	Terrorist	Sabotage, violence

HIGH	Activist/hacktivist	Espionage, data theft, sabotage
	Disgruntled employee	(All of the below)
	Reckless, untrained or distracted employees	Accidental breach or misuse of data
MEDIUM	Thief	Physical theft, espionage, fraud
	Irrational individual	Physical theft or sabotage
	Vendor or partner	Accidental leak, but also intentional fraud or theft
LOW	Outward sympathizer	Deliberate data leak or misuse of data

Source: www.acs.org.au/content/dam/acs/acs-publications/ACS_Cybersecurity_Guide.pdf

Cybersecurity strives to ensure the attainment and maintenance of the security properties of the organization and user's assets against relevant security risks in the cyber environment.

The general security objectives comprise the following (www.itu.int): availability, integrity, which may include authenticity and non-repudiation & confidentiality.

Cybersecurity insurance is designed to mitigate losses from a variety of cyber incidents, including data breaches, business interruption, and network damage. A robust cybersecurity insurance market could help reduce the number of successful cyber-attacks by: (1) promoting the adoption of preventative measures in return for more coverage; and (2) encouraging the implementation of best practices by basing premiums on an insured's level of self-protection (www.dhs.gov).

Financial institutions are looking to take advantage of mobile, cloud, social and other technical trends in order to reignite growth and build customer trust, but must contend with evolving and increasing complex cyber threats.

Cybersecurity refers to preventative methods used to protect information from being stolen, compromised or attacked. It requires an understanding of potential information threats, such as viruses and other malicious code. Evidence shows that a coherent, strategic approach to cyber security can improve an organization's defences and dramatically reduce risk. Pro-active monitoring, continuous analysis, and real-time response are just some of the measures that can make a difference.

Being prepared for a security attack means to have a thorough plan. This plan should include what can happen to prevent the cyber-attack, but also how to minimize the damage if is takes place.

Unfortunately, the statistics reveal that companies are not ready to deal with such critical situations:

-Observing the trend of incidents supported since 2013, there has been little improvement in preparedness in 2015 there was a slight increase in organizations that were unprepared and had no formal plan to respond to incidents; &

-Over the last three years, an average of 77 percent of organizations fall into this category, leaving only 23 percent having some capability to effectively respond.

Most large companies have dramatically strengthened their cybersecurity capabilities over the past five years. Formal processes have been implemented to identify and prioritize IT security risks and develop mitigation strategies, and hundreds of millions of dollars have been dedicated to execute these strategies. Desktop environments are far less "wide open" than they were even five years ago, as USB ports have been disabled and Web mail services blocked. Robust technologies and initiatives have been put in place to address attacks on the perimeter (www.mckinsey.com).

Generally, ensuring digital safety is not easy. That's why there are hundreds of companies around providing numerous products to safeguard consumers and companies from malicious actors. While many of these companies offer seemingly identical products, some of the best are not only protecting users but researching what hackers are doing and exposing them.

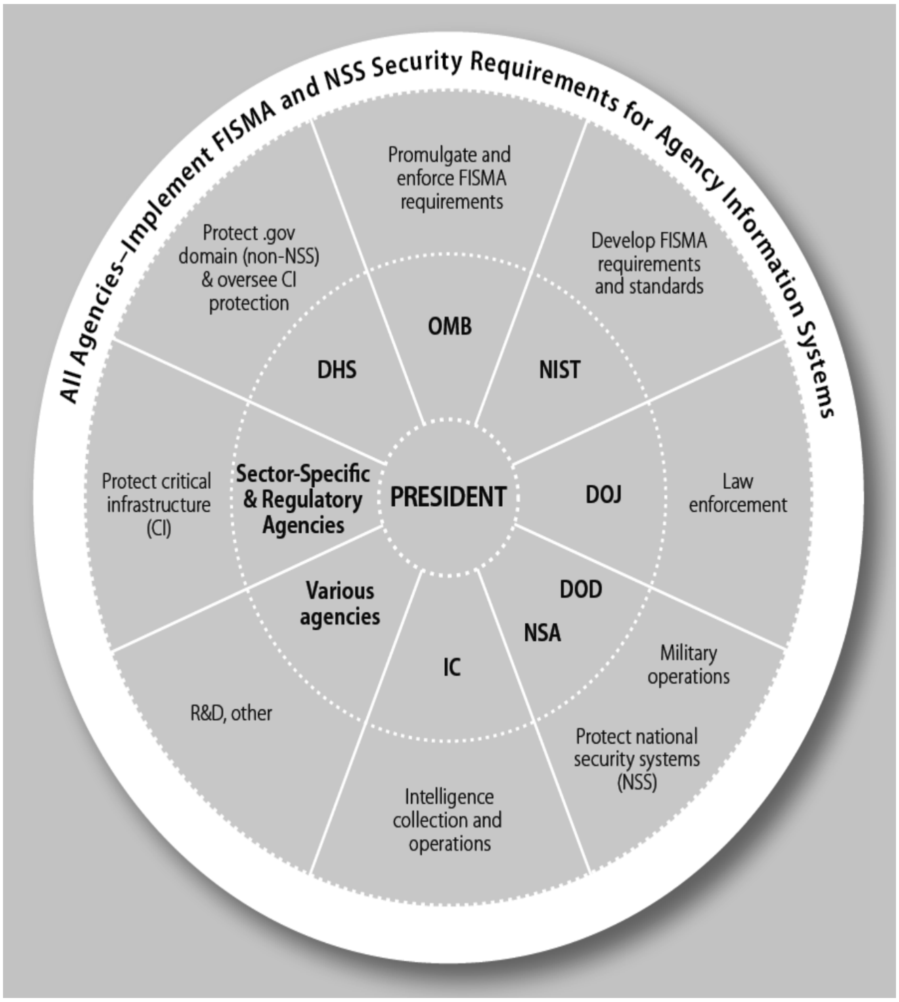
Here are a few of the most influential companies on the market today, and some of the important vulnerabilities they've brought to light (www.businessinsider.com):

1. From the beginning, Kaspersky Lab (founded in 1997) has provided anti-virus software to large companies. But in the 2000s it expanded

to offer more wide-reaching products including consumer and mobile security products. Its researchers have been known to expose some of the most famous hacking groups and their malware. These include Flame — which was discovered in 2012 as a highly advanced cyber espionage program — as well as the Equation group, which was just announced this year as a clandestine computer spying ring;

Figure 2

Simplified Schematic Diagram of Federal Agency Cybersecurity Roles


All Agencies–Implement FISMA and NSS Security Requirements for Agency Information Systems
Promulgate and enforce FISMA requirements
OMB
Develop FISMA requirements and standards
NIST
Protect .gov domain (non-NSS) & oversee CI protection
DHS
Protect critical infrastructure (CI)
Sector-Specific & Regulatory Agencies
PRESIDENT
DOJ
Law enforcement
DOD
NSA
Military operations
Protect national security systems (NSS)
IC
Intelligence collection and operations
Various agencies
R&D, other

Source: https://fas.org/sgp/crs/misc/R43831.pdf

Notes: DHS: Department of Homeland Security; DOD: Department of Defense; DOJ: Department of Justice; FISMA: Federal Information Security Management Act; IC: Intelligence Community; NIST: National Institute of Standards and Technology; NSA: National Security Agency; OMB: Office of Management and Budget; R&D: Research and development.

2. In the world of computer security, the Irvine, California-based Cylance is a somewhat smaller entity. It launched in 2012 and has yet to go public like most of the companies on this list. But in the 2015, the company, which provides anti-malware and threat management using mathematics and machine learning, has made a few very noteworthy discoveries. In 2014, it discovered a very sophisticated Iranian hacking initiative known as Operation Cleaver. And just a month ago Cylance announced a bombshell discovery of a vulnerability in many hotel Wi-Fi setups making both the people on the network surfing the web open to hacking, as well as private networks of the hotels themselves;
3. Cybersecurity firm, Group-IB focuses specifically on cyber-crime and fraud. It has been around since 2003, with customers in more than 25 countries. It claims it is the largest Eastern European forensic lab and "is involved in 80% of all high-profile investigation cases in the field of high-tech crime." In 2014, Group-IB released a report along with the other firm Fox-IT detailing a hacker group known as the Anunak gang, which supposedly wreaked cyber havoc on the Russian banking sector;
4. Trustwave has been around since 1995 and is one of the largest information security companies around. Its research team, SpiderLabs, performs deep forensic investigations and has made a slew of malware discoveries of late. They include a family of point-of-sale malware known as Spark, which is able to steal critical card data, as well as a hacker server in 2013 that contained millions of stolen passwords. Earlier 2015 year Trustwave was acquired by the Singapore company Singtel for $810 million;
5. Avast, which was started in 1988 in the Czech Republic, is one of the largest security vendors in the world. It is most known for its antivirus products, which the company claims its products are used on more than 30% of the non-Chinese consumer PCs.Avast's researchers

have discovered a few well-known security vulnerabilities, including big issues with home Wi-Fi routers as well as one exploit found in numerous Android apps;

6. FireEye is a California-based network security firm. It offers services meant to manage networks for potential threats as well as offer its customers detailed threat intelligence. The company has joined forces with federal authorities, universities, and other security groups to discover and combat various malware. Most recently, FireEye discovered a group of hackers known as FIN4, which was targeting Wall Street to steal insider information; &
7. Founded in 2005, Palo Alto Networks is a network security company known for building advanced firewalls directed toward enterprise customers. Its founder, Nir Zuk, worked as an engineer at Check Point and NetScreen Technologies.Most of Palo Alto Networks' products revolve around network traffic. The company has also made some important malware discoveries, most recently a family of malware known as "WireLurker" that took direct aim at Apple products.

In USA, there are few federal cybersecurity regulations, and the ones that exist focus on specific industries. The three main cybersecurity regulations are the 1996 Health Insurance Portability and Accountability Act (HIPAA), the 1999 Gramm-Leach-Bliley Act, and the 2002 Homeland Security Act, which included the Federal Information Security Management Act (FISMA). These three regulations mandate that healthcare organizations, financial institutions and federal agencies should protect their systems and information.16

In addition to regulation, the federal government has tried to improve cybersecurity by allocating more resources to research and collaborating with the private-sector to write standards. In 2003, the President's National Strategy to Secure Cyberspace made the Department of Homeland Security (DHS) responsible for security recommendations and researching national solutions.

In the United States government, the National Strategy to Secure Cyberspace is a component of the larger National Strategy for Homeland Security. The National Strategy to Secure Cyberspace was drafted by the Department of Homeland Security in reaction to the September 11, 2001 terrorist attacks. Released on February 14, 2003, it offers suggestions, not mandates, to business, academic, and individual users of cyberspace to secure computer systems and networks. It was prepared after a year of research by businesses, universities, and government, and after five months of public comment. The plan advises a number of security practices as well as promotion of cyber security education.

Key Cyber Risk Management Concepts (www.us-cert.gov):

1. Incorporate cyber risks into existing risk management and governance processes. Managing cybersecurity risk as part of an organization's governance, risk management, and business continuity frameworks provides the strategic framework for managing cybersecurity risk throughout the enterprise;
2. Elevate cyber risk management discussions to the CEO. Regular communication between the CEO and those held accountable for managing cyber risks provides awareness of current risks affecting their organization and associated business impact; &
3. Implement industry standards and best practices, don't rely on compliance. A comprehensive cybersecurity program leverages industry standards and best practices to protect systems and detect potential problems, along with processes to be informed of current threats and enable timely response and recovery. Using a risk based approach to apply cybersecurity standards and practices allows for more comprehensive and cost effective management of cyber risks than compliance activities alone.

CYBER SECURITY IN EUROPE

Faced with ever-increasing cyber security challenges, the EU needs to improve awareness of and response to cyber-attacks aimed at member states or EU institutions. The European Union aims to strengthen its cyber security rules in order to tackle the increasing threat posed by cyber-attacks as well as to take advantage of the opportunities of the new digital age (www.consilium.europa.eu).

The most important international convention in the area of cybersecurity is the 2001 Coe Convention on Cybercrime (also called the Budapest

Convention). The CoE Convention is a legal framework of reference for combating cybercrime, including attacks against information systems (www.diplomacy.edu).

The Digital Agenda for Europe (DAE), adopted in May 2010, is one of the most important strategic documents on the EU level that highlighted the shared understanding that trust and security are fundamental preconditions for the wide uptake of ICT and achieving the objectives of the 'smart growth' dimension of the Europe 2020 Strategy.

The directive on network and information security (NIS)18, entering into force in August 2016,requires each member state to establish a Computer Security Incident Response Team (CSIRT) and a competent national authority for NIS, and sets up a cross-EU cooperation group for strategic cooperation as well as a CSIRT Network for operational cooperation, among other provisions.

On 19-20 October 2017, the European Council asked for the adoption of a common approach to EU cyber security following the reform package proposed by the European Commission in September.

This reform aims to build on the measures put in place by the cyber security strategy and its main pillar, the directive on security of network and information systems (the NIS directive). The proposal sets out new initiatives such as (www.consilium.europa.eu):

- Building a stronger EU cyber security agency;
- Introducing an EU-wide cyber security certification scheme; &
- Swiftly implementing the NIS directive.

EU leaders regard cyber security reform as one of the main ongoing aspects on the road to completing the EU digital single market.

- European Council conclusions, 19-20/10/2017;
- Resilience, Deterrence and Defence: Building strong cyber security in Europe (European Commission);&
- Digital single market for Europe.

The EU wants trusted networks as protection against cyber-crime. Threats and opportunities of cyber security (European Commission):

- Security incidents across all industries rose by 38% in 2015;

- 80% of European companies experienced at least one cyber security incident in 2015; &
- 86% of Europeans believe the risk of cyber-crimes is increasing.

Cyber security can enable innovation and help focus on data as the new 'oil of the economy'. Securing Europe's digital future can also mean:

- investing in the use of artificial intelligence and supercomputers in areas such as medical treatments and energy efficiency;
- supporting small and medium-sized enterprises to be competitive in the digital economy; &
- tackling the threats to online platforms and enabling them to make a positive contribution to society.

The costs related to cybercrime and data breaches are thought to be significant and growing fast as digitalization spreads into all spheres of our lives (http://ec.europa.eu).

A 2014 study estimated the economic impact of cybercrime in the Union to stand at 0.41% of EU GDP (i.e. around 55 billion euro) in 2013; with Germany being the most affected Member State (1.6% of GDP). Europol currently estimates the cost at 265 billion euro per year. And the trend is set to rise. A recent study forecasts that the economic cost of data breaches will quadruple by 2019, to reach 2 trillion euro worldwide.

The most affected sectors are financial services, energy, technology, services, industry and defence. At the level of individual companies, various studies relating to French, German and UK-based enterprises have found the economic impact of cybercrime to range from 100,000 euro per year per affected company to as much as 20 million euro, depending on the type of attack. These figures are likely to increase as more and more economic infrastructures become connected.

CYBER SECURITY IN REPUBLIC OF MACEDONIA

Many countries have adopted national cybersecurity strategies and related legislation, taking into account both security and freedoms. A growing number of countries have set up national mechanisms for response to cyber-incidents, involving government as well as the corporate, academic, and

NGO sectors. Some have declared 'cyber' as the fifth military domain, and have set up defensive and offensive cyber-commands within their armies. South-Eastern Europe, and especially the Western Balkans, is lagging behind (www.diplomacy.edu).

The Republic of Macedonia has a relatively modest experience when it comes to cyber security and threats. Simultaneously, considering that Macedonia is a candidate for accession to the EU and NATO, it has to comply with their standards when performing the reforms in the cybersecurity field.

Macedonia has an officially recognized national CIRT known as MARNet-CERT. ITU conducted a CIRT readiness assessment for Macedonia in 2012. Macedonia does not have any officially approved national or sector specific cybersecurity framework for implementing internationally recognized cybersecurity standards.

Specific legislation and regulation related to cybersecurity has been enacted through the following instruments (www.itu.int):

1. Law on Personal Data;
2. Law on Electronic Commerce;
3. Law on Electronic communications;
4. Law on Interception of Communications;
5. Law on free Access to public Information; &
6. Law on Data in Electronic Form and Electronic Signature.

The material provisions related to cybercrime are contained in the Criminal Code and include: endangering safety, violation of the confidentiality of correspondence and other consig nments, misuse of personal data, preventing access to the public information system, copyright violation, infringement of the distribution of technical specially protected signals, audio piracy, child pornography, damage or unauthorized entry into a computer system, development and distribution of computer viruses, computer fraud, making, procuring or selling counterfeiting means, making and using fake credit cards, violation of registered or protected invention and topography of integrated circuits and spread of racist and xenophobic material through computer systems. Additionally, it defines the general terminology regarding cybercrime (https://connections-qj.org).

In terms of institutional capacities to deal with cybercrime issues, the Cybercrime Unit located within the Department for Suppression of Organized and Serious Crime and the Forensic Department of the Ministry of Interior merged into a single Cybercrime and Digital Forensic Department, thus forming a more efficient and effective investigative unit.

Effective response to cyber security treats thus must be comprehensive and highly coordinated among all stakeholders. Consequently this will require response from different stakeholders. So far all of these areas have been addressed by the specific documents in the broader national security context, separate from cyber threats. Therefore nesting the cyber challenges under current Macedonian security strategic documents requires careful analyses of existing legislature regarding the leading national authorities in different areas.

While going after the criminals is important and necessary, more priority should be given to strategies of prevention. It is important, especially in developing countries like Macedonia, to raise awareness of the dangers of unsafe internet usage. Another important aspect would be training of employees. It is crucial that employees, especially those working with sensitive information, have safe working habits that will be regulated with cyber-procedures.

CONCLUSION

The internet continues to create new business and social opportunities that massively scale and widely interconnect. The increasing depth and volume of personal and corporate data make it a more rewarding target for cyber crooks and state-sponsored espionage or sabotage. At the same time, greater connectivity provides more potential attack vectors. As technology advances and the world moves towards an unprecedented use of the internet, the importance of cyber security becomes ever more imperative.

Cyber risk is now firmly at the top of the international agenda as high-profile breaches raise fears that hack attacks and other security failures could endanger the global economy. Cyber-crime costs the global economy over US$400 billion per year, according to estimates by the Center for Strategic and International Studies.

Cyber security is far more than investing in hardware and software. First and foremost, cyber security is a business issue. This means that top management is accountable for ensuring that its organization’s cyber security strategy meets business objectives and is adopted as a strategic risk. Discussions of cyber risk at board level should include identifying which risks to avoid, accept, mitigate or transfer (such as through cyber insurance), as well as reviewing specific plans associated with each approach.

Cyber-attacks fall into two broad categories: breaches in data security and sabotage. Personal data, intellectual property, trade secrets and information relating to bids, mergers and prices are tempting targets for a data security breach. Sabotage can take the form of denial of service attacks, which flood web services with bogus messages, as well as more conventional efforts to disable systems and infrastructure.

REFERENCE:

1. G.Matic and M. Miljkovic, "Critical Infrastructure Protection in Cyberspace", National Critical Infrastructure Protection Regional Perspective, University of Belgrade – Faculty of Securities Studies& Institute for Corporative Securities Studies Ljubljana, Belgrade, December 2013, pp.41-49.
2. Roger A. Grimes, A Data-Driven Computer Security Defense: THE Computer Security Defense You Should Be Using, (Paperback) Roger A. Grimes, 2018.
3. Roger A. Grimes, Hacking the Hacker: Learn From the Experts Who Take Down Hackers, John Wiley & Sons, Inc, 2017.
4. www.businessinsider.com/7-important-cybersecurity-companies-2015-5
5. www.consilium.europa.eu/en/policies/cyber-security
6. www.consilium.europa.eu/en/policies/cyber-security
7. https://connections-qj.org/system/files/3204_macedonia.pdf
8. www.dhs.gov/cybersecurity-insurance
9. www.diplomacy.edu/sites/default/files/Cybersecurity%20in%20 Western%20Balkans.pdf
10. http://ec.europa.eu/epsc/publications/strategic-notes/building-effective-european-cyber-shield_en

11. www.ey.com/Publication/vwLUAssets/EY-cyber-threat-intelligence-how-to-get-ahead-of-cybercrime/$FILE/EY-cyber-threat-intelligence-how-to-get-ahead-of-cybercrime.

12. https://fas.org/sgp/crs/misc/R43831.pdf

13. www.fireeye.com/rs/fireye/images/FE_eBook_Moving%20Targets.pdf

14. www.globalservices.bt.com/.../financial.../Finance_sector_Cyber_Final

15. https://heimdalsecurity.com/blog/10-critical-corporate-cyber-security-risks-a-data-driven-list

16. www.itu.int/en/ITU-T/studygroups/com17/Pages/cybersecurity.aspx

17. www.itu.int/en/ITU D/Cybersecurity/Documents/Country_Profiles/Macedonia.pdf

18. www.mckinsey.com/business-functions/digital-mckinsey/our-insights/meeting-the-cybersecurity-challenge

19. www.surfwatchlabs.com/threat-categories#Actor

UDC 658:339

THEORETICAL VIEW OF GATHERING INFORMATION FROM HUMAN SOURCES IN CORPORATE AFFAIRS

Miroslav D. Stevanović [1], Dragan Ž. Đurđević [2]

[1]*Assistant Professor, National Security Academy, Belgrade*

[2]*Professor, Academy of National Security Republic of Serbia, Belgrade*

This article discusses the collection of information from human sources as an activity in supporting the business of companies. The aim is to determine the characteristics of this cognitive method from the aspect of its role. From the presumption that it is an element of a rational organisation, we analyse it through the necessary arts and functions. It has been established that knowledge from gathering information from human sources is a decision-making factor and that information era imposes new challenges for gathering and protection of data. The results confirm that it is a practical skill, but with the development of a specific subject, method and regularity.

INTRODUCTION

Companies in search of corporate intelligence encompass a variety of entities, including banks, firms, multinationals and law firms (on behalf of their clients). They all seek to grow, by entering new markets, identifying acquisitions, bringing innovations, by advancing their own research efforts. In order to find reliable partners, business entities need to conduct previous research on serious prospects. A new business deal, a new partner inevitably exposes a company to risks. Companies need to make certain they are hiring the right managers and that employees remain alert to the signs of internal or external fraud or corruption. Organizations need geopolitical and competitive assessments. Political, legislative, social or regulatory changes that can affect the business environment, need to be analysed.

Information gathering is a human skill which is required for any organised activity. In order to have information at disposal for any decision-making, it has to be obtained and evaluated in the context of interest. When an entity, like a company, organises purposeful collection of information, it is conducted in a manner which can be described as "aggressive". That means that it involves the extraction of information in direct contact with people, including voluntary (with awareness) and involuntary (without awareness) relationship with potential sources.

In the context of this paper, information gathering is viewed as a process with a distinct purpose to identify and obtain relevant information for successful business operations, security and image of a company.

In this analysis, the term data is used to describe facts, events, transactions, etc. which have been recorded, and which represent input materials in the processing of information. The term information also describes the data, but is used for data that has been produced in a way that benefits the company that is organising its gathering.

Effective corporate gathering of information requires permanent and systemic collection and analysis of a series of information. Collection of information regarding a targeted company is insufficient to provide a complete knowledge framework for rational decision-making.

To ensure a comprehensive result of information gathering, information must be collected beyond that scope, and must include data about comparable and competing companies, the sector as a whole, relevant public stances and administrative relations, as well as the economy and finance in general, but also internal and external personal aspects of a company's functioning. This process can be represented, in essence, as an organised estimation of the potential sources of required information and the practical ways of obtaining them.

The objective of gathering information is an integral part of purposeful efforts to informationally empower the company at the market and society level. It is, therefore, a potential source, like human factor, finances etc., which can facilitate overcoming certain obstacles of successful business operations. In that context, gathering of business intelligence from human sources encompasses two types of collection:

(1) short-term in order to provide input for issues like positioning on the market or increasing revenues (tactical); and

(2) with a focus on longer-term issues such as key risks and opportunities facing the operations (strategic).

In the context of its practical purpose, information can be gathered from public sources. The advantage of this kind of collection is that the sources are generally accessible, and this method does not demand an extra effort to extract information, as it only requires the acquisition of a publication that seeks useful information. This is also a relatively simple and inexpensive, but time-consuming and thus has its application in the company's cognitive process. Practical inadequacy of this method is that much of the information available in public sources may be vague or general and not specific enough.

The purpose of the information collected is its instrumentalisation, through the processing system and establishment of adequate responsiveness. The company managers have their own information relating to their branch of responsibility, but this kind of knowledge is not the kind that is necessarily in an institutionalised form (processed) that as such can be distributed to employees. The function of the planning is to train and encourage managers to make a record of information they have in a way which can be readily used, beyond the level of strategy.

This article looks at the institutionalised and instrumentalised gathering of information from human sources within a company, from the aspect of its internal content. This approach raises several questions:

1. Who is the object of interest and what is the method of information gathering from human sources? Secondly,
2. Is there a specific purpose and role of this collection?
3. What is the practical usefulness of gathering of information?
4. What are the specific arts of information gathering from human sources and
5. What specifics of this activity occur in the information age?

THE OBJECT AND METHOD OF INFORMATION GATHERING FROM HUMAN SOURCES

In contemplating entrepreneurship operations at corporate level, like in the case of institutionalising any other human activitiy that requires overcoming of challenges generated by opposing competative interests (journalism, lawyers, judiciary, diplomacy, etc.), successful functioning and achievement of goals depends on the quality of knowledge about the structure, plans and intentions of other (competing and compatible) interests, enterprises and individuals. Dedication to this objective, on the practical level, can be described as instrumentalisation of network of interactions and influences within a particular category of people (Bean 2011: 43). This results in, as a regularity, the efforts of each stakeholder, including companies, to protect some facts about themselves, and to learn more about the others, or to seek, to find out more in depth information (Prunckun 2013: 34).

These efforts, when conducted by companies, comprise a continuous process through which a company provides necessary monitoring of its industry, market or social surrounding to identify relevant competition, activities, outside affects, responses, and internal issues.

The truth about circumstances, events and relations that are not public or that are guarded in an organised manner can be sought through different ways of collecting segment data (decision-making process, plans, activities, etc.). In this sense, the information obtained (intelligence) is, generally viewed, a product that arises from the process of collecting, comparing, evaluating, analyzing, contextualizing and interpreting the results obtained.

From the aspect of practical application, collecting information from individuals, as the living sources of knowledge, consists of a number of techniques aimed at extracting information of interest for a particular entity from the knowledge that sources were collected or were directly or indirectly available. In that context, collecting information from the knowledge that sources were collected or had direct or indirect disposal of human sources is also a discipline that deals with the rules of dedicated communication with individuals and the human environment in order to directly derive information from them.

The determination to collect information from people represents the purposeful use of communication, i.e. the processing of languages and symbolisms (Neuman 2014: 80), for obtaining their knowledge, predetermines the means of collecting personal contacts with the sources as basic forms of communication. Personal contact, in addition to direct, can be achieved through various forms of indirect communication, including intermediaries, and as an achievement of information age through multimedia.

Methods of collecting information form human sources involves two thought phases. In the first phase, it concerns applying adequate techniques through which information becomes available from natural persons. In the second phase, data are extracted from the obtained knowledge of sources, as well as from other material sources, such as photographs, documents, sound recordings, etc. It does not include industrial espionage, since gathering in this sense uses only legal and ethical means to collect and analyze the available information.

THE ROLE AND GOALS OF COLLECTING DATA FROM HUMAN SOURCES

In order to ensure that the data collected are relevant to fill the gaps in the existing end user's knowledge fund (such as, for example, the entrepreneur in relation to the intentions of a competition in the business, the attitudes of a particular group in the public sphere, various social relations), the collection of data from human sources requires functional management of the entire collection process. Therefore, *ad hoc* acquisition of information related to the issue of interest cannot, as an unorganised form of gathering, be considered as gathering of information in the strict sense.

Ensuring the relevance of information is achieved by structuring the management of the process of gathering, that is, through planned and focused working with the sources and/or the network of sources. The use of human sources provides an opportunity to gain the important data and insights, particularly regarding current data and viewpoints (Murphy, 120), which cannot be obtained by other collection methods.

When these knowledge gaps are adequately filled from resources of human sources, the collector of data (subject of collection) has an opportunity to direct sources about the extent and direction of further cognitive needs (instruction). When data collected are related to the cognitive needs of a company in whose behalf they are being collected, they are forwarded to the competent bodies or managers of that company, either verbally or, more often, in a written form.

The effectiveness of an organised relationship with human sources of information, viewed from the aspect of the goals of extracting information from them, i.e. the relevance, timeliness and accuracy of information on the issue of interest for an organized entity, depends on the harmonious functioning of a series of activities. From those related to the selection and identification of potential sources of knowledge, to organisational support for those engaged in the collection of information. Although collection of information does not necesserily relate to formally classified or otherwise protected information, since it is mainly related to the companies, entities and individuals who have an interest not to disclose certain facts (about their goals, plans etc.), entities in the data collection usually pay special attention to the protection of the identity of its regular and adequately-positioned sources.

Gathering information from human sources has a significant role in identifying rational company's development, activities, politicies, protection of interest, etc, from the aspect of facing behaviour and attitudes of the other existing interests on the market, in the society, or within itself. If the data can be obtained by other means of collection, or from open sources, human sources, as insiders within the scope of interest, it can be kept for the purpose of obtaining information for which there is no other legitimate way of revealing them.

An adequate positioning of a human source implies a higher level of its direct access to will-making and decision-making in a particular environment of interest (development centers, decision-preparing, decision-making or decision-influencing circles, consumer communities etc.) that are required by the decision-makers and managers in the company in whose name and for whose account information is being collected. When the collection of data is required for the needs of a corporate security, or when they are collected by the specialised institutional segments of a company, human sources may even be engaged in endless acquisition of documentation, which can sometimes be an issue from a legal basis if it involves breaching of privacy or protected information.[1]

Gathering information from human sources in the sphere of economy, finance, human resources, public relations, etc., nowadays, is increasingly dependant on the training and abilities of the subject of collection to extract

[1] With wide spread use of mobile phones, capable of phono, video and photo documenting and transmitting communications makes participants in communication are exposed to possibility of willingly or unwillingly leaving a material trace of their knowledge, which may be exploited by the subjects of gathering. Unless such data is legally classified, it is impossible to revert the consequences of their revelation to an interested party.

and obtain the information. This includes various forms of communication and developing relations on the individual or multimedial level, through which subject of gathering can identify the potential source, illuminate ideas and detrimental subjects for the activity of the subjects of study, as well as the intentions and abilities of individuals and groups of other interests on the market. In this sense, collecting information from humans is a tool that, along with other methods of information collection, is applied to obtain the data that fulfill the needs of the company's operations, and may be crossed with other disciplines of gaining knowledge.

The role of the subject of gathering who is in contact with the human source is to collect information from people or from the multimedia and to identify information for the purpose of fully comprehending the truth about the fundamental values relevant for the particular company's enterprises. In this aspect, human sources and various techniques of collection represent the mean of access to data.

Another role of the subject of gathering arises from the most complex aspect of communication with human sources, from the very human nature, since emotions, intentions and motivations differ from person to person and change over time. Because of this, the subject of gathering is a participant with an objective to correctly understand and evaluate the intentions and motivations of the people from whom the information is extracted, as well as the authenticity of the information they provide.

An organized gathering of information implies that those information collected from human sources are necessarily functionally interconnected with those collected through other means. The reason for this is that no position or ability can provide full understanding of the plans and decisions of those who act from the position of opposing interests. In that sense, it represents a part of the cognitive path to advanced analysis for the needs of decision makers (Hall & Citrenbaum 2012).

The key need of analysis is data. As a vital part of a cognitive path, organised storing of gathered data represents more than a statistical tool in the sense that it is an informational resource. Implementing organised collection and analysis of information implies at least two functional developments in a company. Firstly, planning their gathering into data collection as a company affairs, and within this, providing that those who collect the data are systemically involved in the company's planning process. Another stems from the aspect that decisions need supporting evidence, and the reliability analysis of the available information requires a large amounts of data, often collected over a long period of time, and thus it must be provided that gathered data are systematically stored and available for further treatment, evaluation, before their distribution.

FUNCTIONS OF GATHERING INFORMATION FROM HUMAN SOURCES

In the context of the established role and goal, the functions of gathering information from human sources in corporate affairs may,depending on the immediacy of access to the primary data, be distinguished, in principle, as extractive (gathering in the narrow sense) and derivative (gathering in the broader sense, analysis).

In the function of gathering in the narrow sense, depending on whether the human source is assessed as generally friendly or generally hostile towards the goal of the subject of gathering, data can be obtained with the use of various techniques of interpersonal communication:

- through systematic direct and personal questioning of an individual which is, by indirect verification techniques (verbal provocation), stimulated into verbal reactions that contain empirical data that give an answer to the specific cognitive needs of the examiner (interview).

This kind of inquiring implies a situation in which the interviewee (potential source) is not aware of the goal of the conversation, which imposes the need for the subject of gathering be well priorly prepared. This situation also restricts the circle of potential interlocutors, in the sense that questioning through an interview can only be conducted with sources that are estimated to be friendly or neutral in relation to the target of the subject of gathering.[2] This type of questioning has application, for example, in the sincerity check of the source, or checking the existing data

- through non-systematic discussion by providing indirect incentive techniques, i.e. introducing information that provides indications of the

[2] Formally, the interview can also be applied to an antagonistic source, and especially if it is prepared to compromise. However, since it is an indirect testing technique, such application is risky from the point of view of revealing the knowledge and interest of the subject of gathering, and can lead to the reluctance of the potential human source.

position and priority of the source (survey), according to a sample priorly established according to the probability that the source has access to relevant data and the degree of difficulty of extracting information (for example, consumer preferences in front of a supermarket, attitudes of the passers-by to the advertising campaign, etc.).

This technique of conversation, strictly speaking, does not represent a method of data gathering, but it can be applied when there is a need for quick access to information, in order to evaluate and select human resources for collection, product relations, and assessment of opinion. The similarity with the interview is the superficial friendly relationship of the source and his lack of knowledge of the subject of the test. The main difference is that it can be an introduction to further contacts.

- through tactically-oriented techniques of organised data-extraction from sources who knowingly provide information on individuals, ideas and activities, intentions, tactics and abilities and strategies of stakeholders and groups that pose challenges for the entity in whose name data are being collected.

This technique is a way to get timely information and, in principle, it is done primarily by direct encouragement, and, if necessary, by using the elements of investigating and interviewing.

- through tactical questioning of individuals who can or on their own initiative provide information that can provide information relevant to understanding a particular situation.

This, test-technique, is applied, similarly to the survey, for the expeditious initial data gathering of direct value using immediate tactics of the company. On the other hand, if the human source delivers the knowledge using his own initiative, there is a similarity to techniques of collecting for tactical purposes, in the sense that it also allows direct incentives of subject of gathering.

- through systematic extraction of information from media formats, in accordance with the needs of data collection (exploitation of documents).

This technique is developing in parallel with information technologies and essentially represents indirect collection from human sources in the broader sense, and therefore is part of the management of the process of data gathering.

- through systematic efforts to obtain data that allow responding to the specific need for data collection, by using techniques of direct and indirect questioning of individuals who are under a state of compulsory presence (similar to interrogation).
- through meeting with representatives of other entities involved in the collection of information.[3]

This is a type of systematic conversation in which subject of gathering not only seeks to obtain information and data by indirect and direct incentive techniques, but also to establish coordination or reduce the risk of direct confrontation in the activity.

Gathering of data and information from human sources in the function of analysis, includes identification of the following:

- trends, in a way that the subject of gathering seeks to focus on the needs for the support of the specific current opeations of the company on whose behalf data are being collected (for example, the sale of a particular product, the completion of research, the acquisition of a job);
- patterns, in a way that the subject of gathering seeks to provide information necessary to identify the intentions, capabilities, dispositions and influence of the entity or individual that are the object of research; and
- analytical tools, in a way that the subject of gathering combines available knowledge with unified and strategic analysis, to assess further development.

The product of collecting information from human sources consists, on the tactical level, of information about the object of interest, its collisions with the interests of the company in whose name data are being collected, assessing the weaknesses of the objects of interest. The final information, derived from data collected from human sources, is strategically merged, on the company level, in the form of a database, an assessment, or an analysis. These bases can refer to activities of the competition on the market, business operation, financial operations, risk factors, insight into ideas and conceptual solutions, research and development, as well as on different interests

[3] This category of individuals includes representatives of competing or antagonistic companies, information institutions, marketing agencies, financial institutions, non-governmental organizations and other organized entities, as well as various informally organized social groups.

in public and private sector (Hulnick 2014: 50-51), which do not have to be based on law.

Efforts by people seeking information become standardised as companies' hunger for data grows in the contemporary business surrounding, and develops into a professional engagement in organised search for usable sources of data. Enterprises gather and collect data inside and outside of their own organizations. In that context, it should be noted that some of them may be obtained through interested parties, like brokers, bankers, etc. but even though they may seem helpful, they do not necessarily serve the purpose of the company, and thus have to be analysed through internal mechanisms, in order to be disseminated or taken into account for decision making.

Proper knowledge, skills and analytical support are a prerequisite for the available and obtained data to be reliably and effectively used for operations like investing, planning, or other market operations. External data, i.e. information that is not in posession of the company, may include unstructured data as well as those in posession of other entities. They include data on organisational issues, attitudes, individual will, plans, intentions etc. These are most appropriately delivered by insiders or well-informed human sources. Therefore, companies increasingly attempt to organise their own gathering of data.

In contemporary information surrounding, a large amount of information, especially those related to human resources (Burrow, Kleindl, 2013, 18), are processed by various software or online solution, which enables fast entry, tracking, and recalling of informational needs, human sources, payroll, management, and accounting functions within a company. Basically, availability of relevant information is functionalised at the highest level of management, as this is the place of convergence of all processes within the company, and requires objectivity and a realistic approach to a quick reaction to the outside world.

Certain information, due to its nature, can be obtained solely or most efficiently through human sources. As for conducting business, this information has two primary functions:

(1) the problem solving level

An example of using information on problem solving level are the situations in which an external information is needed for evaluating or assessing the market.

(2) the level of strategic or action planning

An example of its use at the planning level are the situations in which some information is related to the competition's product development, shifts in market, performance of certain critical company, and industry trends. General role of gathering information is to facilitate anticipation of challenges and conditions and awareness of changes and possibilities. Fundamentally, the information is in function of providing a basis for dealing with general dilemmas of decision making, what the current status is and what the perspective is.

It is important to note that not all information gathered from human sources should be considered as a good practice of the company. The emergence of an organised attempt to reveal another company's confidential data about products and campaigns, or collecting in clandestine manner (secret documenting) provides legal action against companies which engage in such practices. Also, a debriefing about company's businesses in which state actors are involved cannot be considered as a legal business practice (Roper, 2014, 105).

Another note worth mentioning is about private gathering of informal information (intelligence), usually by managers, about practices of other companies or employees (Snell, Bohlander, 2013, 75). This is, to some extent, unavoidable, since it is partly a consequence of natural flow of information, but should not be treated as a useful practice, since it does not provide an objective account, but rather a personalised and biased one.

Companies should, since the information they obtain is in the interest of an entity as such, at least instruct the employees in ways they could be of assistance in gathering information from human sources (Halibozek, Kovacich, 2005, 97).

By seeking information that is not publicly available, the subject of information gathering may develop an insight of what the key players are and what the stakeholders really think, and may assist in anticipation of the plans. The goal is to obtain data that will help in overcoming the challenges that can undermine the company's operations. An intelligence-gathering program is not a guarantee against disruptions, but it enables companies to identify gaps and find the best route in following their own interests in a real environment. Gathering information from human sources, at the basic level, is conducted with an objective to facilitate transformation of data for the purpose of the company's worthwhile goals.

THE SKILL OF GATHERING INFORMATION FROM HUMAN SOURCES

The various types of data collected in economic, social, environmental, cultural and financial spheres provide information of relevance for rational decision-making. Most of the data consists of facts that are widely or publicly available, and therefore gathering information from human sources is generally done openly, except for specialised discrete gathering by corporate security and/management of companies.

Important types of 'data' can be derived from the type of knowledge acquired through techniques of their extraction from human sources in a narrow sense. It concerns a certain phenomenon, relationship, or condition that foremost has its external manifestation. The issue of perception must have a meaning that can be determined. Finally, the information obtained must have a place in the process of thinking. In this context, the data represents at least double perception, of the source and of the subject of gathering.

Linguistic and symbolic nature of the techniques of gathering information from human sources conditions the subject of collection to apply a set of principles from different disciplines, from psychology, neuropsychology, sociology, and so on. All of them are conveyed through an external manifestation. Namely, linguistic and symbolic communication is used in a function to stimulate the potential source of information to react. In a narrow sense, verbal response to a desired topic can be achieved by direct or indirect incentives, questions, or statements with inquisitive or open sense.

Depending on the assessment of the subject of gathering regarding the structure of the personality of the human source, it is possible to distinguish three types of incentives, which can be made verbally, literally and/or symbolicaly applied to a potential source: (a) mildly, (b) neutrally and (c) sharply.

Depending on the circle of the person with whom subjects of gathering communicate, these incentives can be applied personally, which is the most common practice, but also in groups and collectively. The subject of gathering can perform individually, or within a team (two or more collectors, with established roles and assigneents).

The techniques of gathering data generally imply oral and personal communication, directly or through multimedia. Therefore, gathering necessarily implies a relationship of two personality structures. On the one hand, there is the subject of gathering, whose position depends on the dominance, in terms of prior awareness of the purpose and nature of communication. On the other hand, there is a potential human source, whose elements of supremacy exist in terms of the consent, the place, the time and the content of communication, the form of response and the atmosphere of communication, which subject of gathering attempts to overcome (Nešković 2015: 9).

Overcoming of the elements of the superiority of the potential source by the subject of gathering requires, depending on the goal, the assessment of the structure of the personality of the potential source and circumstances, application of techniques of direct (indirect) or indirect (unreasonable) incentives (questions or open content), individual or team appearance, orally or in writing, survey or interview (Merriam 2009: .90-91).

In accordance with the challenge faced, the communication strategy, from the aspect of extracting information, includes two dimensions: on the one hand, the conduct of the subject of gathering is aimed at overcoming the possible psychological barriers of the potential source (psychological dimension)[4] and, on the other hand, the organisation of communication content (logical dimension)[5].

A particular segment of indirect incentive, to which the subjects of gathering often have to resort, is the application of techniques of questions that do not appear offensive to the consciousness of the potential human source. These techniques include: valuable statements, which lead the potential source in a particular direction (suggestive); statements about possible behavior of others (projected); and leading the potential source to explicate personal views on the imaginary situation (hypothetical).

Gathering information from human sources is organised as part of a regular company's activities. This implies that subjects of information gath-

[4] The psychological dimension includes the adaptation of elements such as, the introductory questions and their further order, the rhythm and duration of the examination, the presence and participation of others, the forms and the tone of the issue, as well as other elements in order to achieve the growth of openness and sincerity.

[5] The logical dimension involves the determination of questioning, from general to more specific questions, or to defining the basic and surrounding issues that explain it, or their combinations in order to discover the content of the statement of the potential human source of information.

ering must have an activel approach and full commitment, both in terms of planning and execution, as well as continuous availability to the potential sources and presence in environments where potential sources can be found (OHCHR, 2011).

A special concert, as a company's activity, is maintaining ethical conduct, since it is related not only to the reputation of a professional who is extracting informtion but also of the company. Namely, honest, discrete, professional and ethical approach to extracting information is more likely to strengthen the interpersonal relationship with specific source and potential human sources.

In the context of active relationship and commitment, the process of organised gathering is also characterised by the fact that information is extracted directly or in a verifiable manner, which demands professional competence of those who collect them (Crump 2015: 137-139). because of the limitation of the results obtained from human sources in relation to the need for accurate qualitative data, professional competence includes the skills to obtain as much valid information as possible. This skill involves art especially in asking questions in such a way that the object of acquiring feels free to respond, as well as listening to the interlocutor, which requires practical experience (Thomas 2015: 298). The outcome of experience in this art leads to confidence building of professional subjects of information gathering (Prunckun 2012: 260).

The skill of gathering information from human sources as a company endvous represents focused collection and analysis of all data concerning an unfamiliar subject, issue or relation, that is used as a key insights for decision makers in support of a certain major company concern or action.

On the practical level, the art of gathering information from human sources involves certain routines, necessary to enable continuous work of professionals and overcoming of possible distractions. These can be summed up as follows:

- identifying goals of each contact
- recognising various types of conversation handling
- planning and preparation for conversation
- quality of communication (verbal, non.verbal) skills
- asking key questions in logical sequence
- breaking-up answers during conversation

- extracting reliable and correct data (by predetermined criteria)
- taking notes or recording
- making a report

COLLECTING INFORMATION FROM HUMAN SOURCES IN INFORMATION AGE

Gathering information from human sources is sometimes perceived in public as secret espionage, although in reality most subjects of collecting perform their work publicly (Goldman 2015: 187) and most often in accordance with the laws. Until the technological revolution at the end of the twentieth century, gathering from human sources was the primary source of information. Today, this method is affirmed as a way to openly gain insight about other entities, relations and individuals in many areas of life (Gerdes 2004: 159). In the situation when, due to the volume and speed of the available data, it is increasingly difficult for decision-makers to perceive changes and trends (Kayes 2015: 57); it seems rational to expect that the importance of insider information will not be lost in the process of ensuring rational decision-making.

The explosion of information technologies has not suppressed information collecting from human sources, even in agencies that deal with secret data collection (Dupont 2003: 21). There seems to be at least four essential reasons for this. Firstly, because in this way information is obtained that technologies cannot transfer, such as an access to internal decisions, or internal relations within the data collecting entity. Secondly, a human insight can provide information about intentions, while technical collection is generally limited to determining abilities. Thirdly, collecting from human sources can be used to find out plans before their realisation is initiated. Finally, this method of collecting data includes selecting and identifying potential sources and conducting various conversations (Girod 2014: 9), and thus does not require much logistical support and is cost-effective compared to technology.

The information age has provided a new dimension in gathering information from humans. The development of communication on the Internet has led to the development of a platform for automatic lexical and functional processing of information from open sources, and with it the analytical assessment about the relevance, reliability and credibility of participants in the global network. This possibility is found in target scrolling in order to establish relevant contacts (essentially direct) on social networks (Baldini 2007: 331-333).

The adaptation of gathering of information from human sources for use in virtual space has also imposed a need to search a vast amount of information, which has transformed data collection into continuous data hunting (mining) and making it additionally complicated decision-making (Olcott 2012: 234-235).

From the aspect of the objective of gathering information from living sources, structural changes in the decision-making process are interesting to observe, in terms of the management systems that generate the information age. Namely, the data are collected for the purpose of rational decision-making in the sense that provides a comparative advantage for the entity that seeks to ensure it. This implies that the entity on which data is collected, certain operation on the physical market, determines the comparative advantages.

In the case of international or transnational companies, corporations and business systems, local information gathering has no impact on their centre of operations. The resilience of this category of entities rests on their ability to shift the focus of their decision-making to places where there is no resistance to their interests, along with the ability to adapt to the physical space. Hence, the opposing interest group does not benefit from local informative influence (including on national level), even though the best-positioned human sources, because territory is not practically important for their decision-making capacity (Autonomedia, 1996).

In the information age, the collection of intelligence is a prerequisite for running or conducting a successful corporate project or a plan. Thus, new communication technologies and new applications of information and intelligence change the general conduct corporations, and therefore induce a greater need to face a challenge of anticipating these changes in an organised way.

CONCLUSION

It is generally accepted that in the organised decision-making process of every company, and especially in the technological age, a manager needs information in order to find suppliers, mobilise capital, win customers and neutralise rivals. Gathering information, in this context, from human sources does not mean leaving its acquisition in an unplanned, instinctive process.

From the aspect of its practical application, information gathering from human sources undoubtedly constitutes a skill necessary for successful management of the company's affairs. However, the examination of its organised aspect shows that this skill, even though it requires a multidisciplinary approach, has its internal regularities and procedures both in terms of source selection, and in terms of communication with the source.

Collecting data from human sources is a consequence of inevitable struggle and competition for survival and success of organised entities and in this respect, it is limited only by the law and efforts of competing entities to preserve data about influences on their decision-making process. Hence, functionally, successful implementation of this activity in company's affairs, which is now included in the organisational structure of many companies, does not depend only on the art of the subject of gathering, but also on the application in practice of theoretical achievements in the fields of many disciplines, which besides economy and finances, includes psychology, neuropsychology, anthropology, sociology and others.

It is widely known that copyrights, corporate secrets and surveys are protected at national and international level, but when it comes to information gathering, this obstacle is ineffective because, as we have shown, the intentions, plans and will of decision makers are elements of an organization that cannot be protected because they reflect the quality of the system organization. For this reason, information gathering regarding these aspects does not violate the rules which protect intellectual property and does not constitute unlawful conduct. In support of this, it can be noted that gathering form human sources is without opposition implemented by law firms and various international missions.

The fact that information gathering is a widespread and based on survival (on-market) of companies which have a more adequate organisational decision-making mechanisms, indicates that the necessary knowledge of its techniques, role, scope and prevention should be an integral part of the education and training for corporate management. The basic argument in favour of this is that, in the era of mass and rapid communication, the capacity of a company to function and achieve its goals depends on the ability to face obstacles and survival, and the prerequisite for this is the willingness to deal with competition and opposing interests, including employees at all levels.

It seems undisputable that methods of gathering and analysing intelligence from human sources have a place in the organisation of a company. What should be recognised is that the methods used to collect business-related intelligence are by nature such so that the company may succeed in its business. They are different from similar methods used by government intelligence agencies in a way that they are not intended for use, and only guided by reckless interest, but should be sufficient for loyal and illegal competition. The distinguishing line is that company intelligence gathering methods are expected to be legally adapted to the world of business, which faces an increasing number of closed doors, less willing sources, and greater reliance on personal communication skills.

Gathering information from human sources, as shown, relies on systematic gathering, analysing and interpretation of data in support of a business' strategic plans. Its practical content involves reading documents, tracking market trends and legislation, making discreet inquires, using search engines and online archives, and speaking with suppliers, competitors and customers. What makes this skill specific is the overall objective, and that is the improvement (rationalise) of the quality and outcome of the company's business decisions.

Bearing in mind the methodological demands, we can determine specific skills of the company's professional subjects of information gathering from human sources that can be taught and trained. These, in addition to the fluency in technical skills and essential importance in the information age, require two skills that enable leading of the business and other people by using available insights. One can be described as the ability to adopt a different perspective or mindset. The other, as already mentioned, is the communication skill, which should always be developed through special training.

REFERENCES

Autonomedia (1996). Critical Art Ensemble, *Electronic Civil Disobedience and Other Unpopular Ideas & Other Unpopular Ideas*, New York: Autonomedia. Retrieved: http://www.critical-art.net/books/ecd/ (Accessed 3. January 2018).

Baldini, N et al. (2007), A Multilanguage Platform for Open Source Intelligence, in: *Data Mining VIII: Data, Text and Web Mining and Their Business Applications*, A. Zanasi et al. (eds.), Southampton: WIT Press.

Bean, Hamilton (2011), *No More Secrets: Open Source Information and the Reshaping of U.S. Intelligence: Open Source Information and the Reshaping of U.S. Intelligence*, Santa Barbara: ABC-CLIO.

Crump, Justin (2015), *Corporate Security Intelligence and Strategic Decision Making*, Boca Raton: CRC Press.

Dupont, Alan (2003), Intelligence for the Twenty-first Century, in: *Twenty-First Century Intelligence*, Wark, Wesley (ed.), Oxon: Routledge.

Gerdes, Louise (2004), *Espionage and Intelligence Gathering*, Farmington Hills: Greenhaven Press.

Girod, Robert (2014), *Advanced Criminal Investigations and Intelligence Operations: Tradecraft Methods, Practices, Tactics, and Techniques*, Boca Raton/London: CRC Press.

Goldman, Jan (ed.) (2015), *The Central Intelligence Agency: An Encyclopedia of Covert Ops, Intelligence Gathering, and Spies: An Encyclopedia of Covert Ops, Intelligence Gathering, and Spies*, Santa Barbara: ABC-CLIO.

Hall, Wayne Michael; Citrenbaum, Gary (2012), *Intelligence Collection: How To Plan and Execute Intelligence Collection In Complex Environments*, Santa Barbara: ABC-CLIO.

Hulnick, Arthur (2014), The Future of Intelligence: The of the Intelligence Cycle, in: *The Future of Intelligence: Challenges in the 21st Century*, Duyvesteyn, Isabelle; de Jong, Ben; van Reijn, Joop (eds.), London/New York: Routledge.

Halibozek, E., Kovacich, Gerald L. (2005), *Mergers and Acquisitions Security: Corporate Restructuring and Security Management*, Brlington: Elsevier.

Burrow, James L. Kleindl, Brad (2013), *Business Management*, Mason: Cangege Learning.

Kayes, Christopher (2015), *Organizational Resilience: How Learning Sustains Organizations in Crisis, Disaster, and Breakdown*, Oxford: Oxford University Press.

Merriam, Sharan (2009), *Qualitative Research: A Guide to Design and Implementation*, San Francisco: Jossey-Bass.

Murphy, C. (2016). *Competitive Intelligence: Gathering, Analysing and Putting it to Work.*

Oxon/New York: Routledge.

Nešković, Slobodan (2015), Mogućnosti implementacije tehnika prikupljanja podataka u konzularnim poslovima, *Pravo – teorija i praksa*, 10–12/2015.

Neuman, Yair (2014), *Introduction to Computational Cultural Psychology*, Cambridge: Cambridge University Press.

OHCHR (2011), *Manual on Human Rights Monitoring*, 2nd edition, Geneva: Office of UN High Commissioner for Human Rights, (internet) Retrieved: http://www.ohchr.org/Documents/ Publications/Chapter07-24pp.pdf (Accessed 3. January 2018).

Olcott, Anthony (2012), *Open Source Intelligence in a Networked World*, London/New York: A&C Black.

Prunckun, Hank (2012), *Counterintelligence Theory and Practice*, Lanham: Rowman & Littlefield.

Prunckun, Hank (2013), *Intelligence and Private Investigation: Developing Sophisticated Methods for Conducting Inquiries*, Springfield: Charles Thomas Publisher.

Roper, C. (2014), *Trade Secret Theft, Industrial Espionage, and the China Threat,* Boca Raton: CRC Press.

Snell S.A.,↱Bohlander G.W. (2013), *Managing Human Resources*, 16th edition, masn: Cengage Learning.

The CIA National Clandestine Service (2010). Historical Document, 21.10.2010. Retrieved: https://www.cia.gov/news-information/featured-story-archive/2010-featured-story-archive/intelligence-human-intelligence.html (Accessed: 3. January 2018).

Thomas, Jerry et al. (2015), *Research Methods in Physical Activity*, 7th edition, Champaign: Human Kinetics.

UDC 005.334:334.72

SOCIAL ENGINEERING: A BIG CORPORATIVE SECURITY CHALLENGE

Nenad Taneski[1], Toni Naumovski[2], Ferdinand Odjakov[3]

[1]PhD, Assistant professor, Head of the Department of Military Science,
Military Academy/MoD
[2]PhD, Staff officer in General Staff,
Army of the Republic of Macedonia /MoD
[3]PhD, administrative servant /MoD
Military Academy "General Mihailo Apostolski", Skopje

The human approach, often social engineering termed, is very present in the era of modern business and globalization. In other words, social engineering is referred to as 'human hacking'. It uses trickery and deception to take advantage of human behaviour. The globalization has changed the structure and pace of corporate life and the malicious activities are used to breach the information security defences of the corporations. It is perhaps the most powerful tool that harmed corporations and it is based on the plethora acts of unfair business competition. Social engineers use different manipulating technics to accomplish the goals, so the most popular guidelines for internet interaction are: 'be suspicious of pop-up warnings'; 'don't use the same password for multiple applications or websites. Ensure they are a mix of letters and numbers and change them often'. There are multiple ways to combat social engineering attacks and one is Public Key Infrastructure -PKI. This paper analyses the social engineering as a big corporative security challenge. The focus is on the categories of the social engineering and paper highlights the importance of providing key information security capabilities, by using PKI. The paper is intended to cover the challenges of social engineering and should provoke additional discussion and research.

INTRODUCTION

Social engineering is becoming a bigger and more complex security threat that corporations must take seriously. Many unfair manipulated activities target the human weakness and vulnerabilities. The types of information that social engineers are seeking can be different, but when employees are targeted, the social engineers are usually trying to deceive into giving them confidential information. They also be trying to access to the computer system of targeted corporation to secretly install malicious software, which will give them control over the system and allow them access to the needed information. So, social engineering, aimed to gain access to the system of any organization despite the different ways of security controls and policies. That access is nothing else than deception and it could be possible in two main ways: **human and computer based**. The biggest threat to the security of the corporation is not a weakness of the computer system and technology. Actually the biggest threat could be the employees and their naivety. As the internet expanding continues to increase, the threat of social engineering also increases. Corporative security is very linked with the challenges deriving from the social engineering. The technical aspect of the corporative security made much progress in recent years. On the other hand the social engineers are more sophisticated than ever and became more adept at attacking. They are able to hold corporations as hostage, or to damage their security system. For many corporations the weakness thread for the security is now the **human**. One of the typical social engineering attacks is phishing, which attempt to acquire sensitive information from the employer and with that he is a potential victim of a fraud. Combating social engineering is most effective as a layered approach. PKI is one of the layers. Security of confidential information should be a fundamental part of the corporative security. So it is important to understand the importance of the social engineering as a threat, and the ways of its manifestation.

DEFINING SOCIAL ENGINEERING

According to Oosterloo (2008) social engineering is *the successful or unsuccessful attempts to influence a person(s) into either revealing information or acting in a manner that would result in unauthorized access to, unauthorized use of, or unauthorized disclosure of an information system, a network or* *data*. Social engineering is focused on human behaviour. Despite the technical aspects of corporative security where is achieved a large improvements, the same cannot be said for the human factor of corporative security. So, the focus has been shift to the employees of the corporation. Social engineering is the 'art' of utilizing human behaviour to breach security without the participant (or victim) even realizing that they have been manipulated (Gulati, 2003:1). Gulati points out that the ultimate security wall is the human being, and if that person is duped, the gates are wide open for the intruder to take control. Actually, the employees are unaware of the value of the available information and therefore do not care about their protection. Human nature is the basis of every social engineering attack. So the ignorance of the social engineering and its effects make the corporation vulnerable and easy target. According to Cortez (2013) social engineers lure people to divulge information by promising something for nothing. Common targets of social engineering include users, receptionist, help desk personnel, executives, and system administrators. Other targets include insiders with criminal backgrounds and terminated employees. There are many factors that make the corporations vulnerable of social engineering such as insufficient education and training in the field of information security, insufficient security policies and easy access to the information, as well as huge and complex organizational structure. Security policies are effective as long as the weakest link is strong. Actually the employees are the most sensitive. Attackers and defenders are constantly playing cat and mouse. Defenders try to stay ahead of attackers' methods, and attackers are always coming up with new ways to strike. This back and forth will only continue (Ablon, 2015). There is no unique method that will ensure complete security against attack of social engineering. The types of attacks can vary, but when individuals/employees are targeted the social engineers usually, by trick, tries to get confidential information, or to get access to the company network or computer system, to secretly install malicious software-that will give them access to the passwords or other confidential information as well as giving them control over the corporation network or computer system. The access to the corporation network or computer resources is often due to the natural human tendency for helpfulness. In addition, the social engineers may try to exploit the employee's lack of knowledge and also the rapid development of technology. Many employees do not realize the full value of personal data and are unsure how to protect confidential information. Any company, government, individual, or power can be destroyed due to a lack of knowledge (Evans, 2009:1). Evans (2009:12-13) states that social engineering is the exploitation of said vulnerability and there is no patch for human stupidity. It is a problem with no solution. About the nature of social engineering, according to Evans, the psychological aspect of social engineering is what makes the attack, not the technical.

MANIFESTATION OF SOCIAL ENGINEERING

Each social engineering attack is unique, with the possibility that it might involve multiple phases/cycles and/or may even incorporate the use of other more traditional attack techniques to achieve the desired end result (Malcolm, 2007:5). As social engineers are closely related to hackers, their overall motivation and personal motives are the same Oosterloo (2008). Following information has been identified as useful, by Oosterloo (2008), for the social engineer and should be classified as such:

- Gathered information:

✓ Organizational structure,
✓ Employee names,
✓ Employee functions,
✓ New employees,
✓ Calendars,
✓ Internal phone numbers,
✓ E-mail addresses,
✓ Organizational policy and processes,
✓ Lingo,
✓ IT infrastructure,
✓ Organizational logos,
✓ User names,
✓ Passwords,
✓ Server names,
✓ Application names,
✓ Manuals,
✓ IP addresses.

There are two main categories which classified social engineering: **human based** social engineering and **computer or technology based** social engineering. Gulati (2003:1) explains these two categories of social engineering. According to Gulati, the human approach is done through deception, by taking advantage of the victim's ignorance, and the natural human inclination to be helpful and liked. On the other hand, the technology based approach is to deceive the user into believing that he is interacting with the 'real' computer system and get him to provide confidential information. The intent of the attacker is to access to the network and the computer system of the corporation. In the case of human based social engineering, usually the attacker, after the research on the target company, try to identify frustrated disgruntled employee/employees, to develop relationship with the employee/employees and exploit the relationship (Cortez, 2013). The attacker tries to collect sensitive information by interacting with the victim. The attacks exploit the trust and the human nature to help. Figure 1 presented the attack cycle.

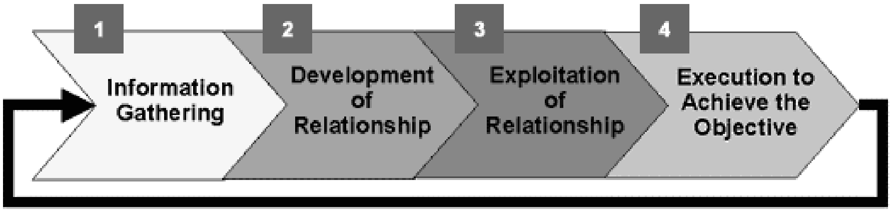

1
Information Gathering
2
Development of Relationship
3
Exploitation of Relationship
4
Execution to Achieve the Objective

Figure 1: Human based social engineering attack Cycle

This descriptive cycle is frequently used both by security professionals and academics when describing social engineering attacks. But the model does not provide any suggestions for proper protection, making the model of limited use (Kohlberg and Kowalski, 2008:2).

Kohlberg and Kowalski (2008:2-10) develop a new model of the social engineering attack cycle describing attacker, defender, and the victim and merge them into a model describing the cycle of deception (Figure 2). In the model they emphasized that if the attacker is unable to hide the attack, he will most likely get caught, and if the internal rationalization of the attacker does not judge the attack as a 'good' experience, he will most likely not continue. Kohlberg and Kowalski points out that the same is true of the defender.

If any one of the steps in the defence cycle is good enough to stop the attacker, then the attack will obviously fail or let the attacker be caught. The victim is submitted in each of the sections in the model. Actually the model covers activities by all involved-victims, attackers, and the protecting organization. Attackers get their chance due to weaknesses found in people. These could be because behaviours due to trust or ignorance but could also be through simpler persuasion or manipulation.

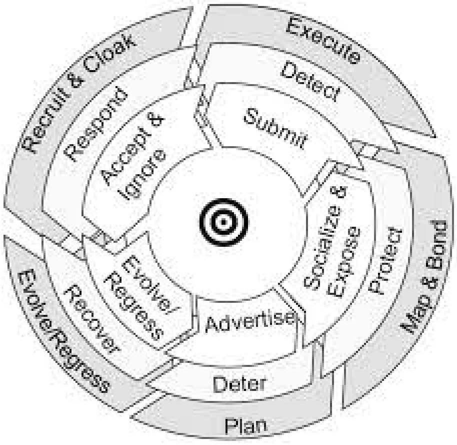
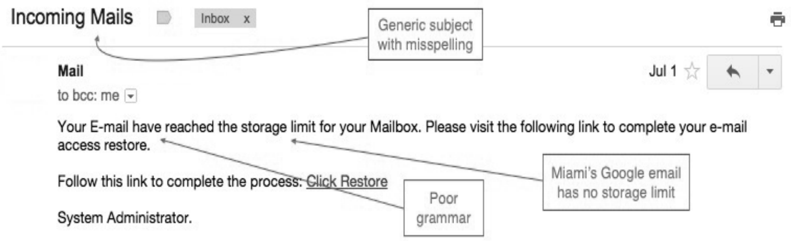


Figure 2: The cycle of deception

There are several models of the social engineering attack structure available, but none was complete Oosterloo (2008). Common for all is interaction between preparation, manipulation, exploitation and execution.

It is generally much easier to trick a person then it is to trick a complex computer. Social engineering across information technology networks is a fairly new idea. With all new ideas come new questions (Evans, 2009:62). These questions are related to the computer based social engineering. More people are connected to and interact with technology, whether they want to or not, and they aren't necessarily security-aware. This makes their digital world easier to target and access (Ablon, 2015). Ablon in the context of computer based social engineering says that the social engineering is often the first step in malicious hacking. It often enables attackers to gain physical access to a target's devices and networks, and facilitates the gathering and harvesting of credentials (such as username/password combos) for follow-on network-based attacks (such as installing malware on the network or stealing intellectual property). Ablon emphasizes the fact that according to 2015 Symantec report five of every six large companies had been targeted by spear-phishing attacks in 2014. Phishing is one of the biggest computer based social engineering techniques that attackers use to infiltrate companies. Through phishing, a potential hacker tries to acquire such information as usernames, passwords, and financial or other sensitive information. Ablon explains the spear phishing, where the 'bait' is directed at a specific individual or company. Customizing the attack increases the probability that the victim will fall for the spear-phishing campaign. Phishing uses specially crafted emails to entice recipients to visit a counterfeit website. This website is likely to have been designed, using well-known and trusted brands, to convince the individual to provide financial and/or personal information. The information harvested is then used for fraudulent purposes (Malcolm, 2007:8). Phishing is a message falsely representing that it is legitimate website and attempts to collect personal information and detailed information of a bank account. Figure 3 represents the possible indicators in the message that pointing to phishing. It could be misspelling, inconsistencies in the message, poor grammar.



Your E-mail have reached the storage limit for your Mailbox. Please visit the following link to complete your e-mail access restore.

Follow this link to complete the process: Click Restore

System Administrator.

Generic subject with misspelling

Miami's Google email has no storage limit

Poor grammar

Figure 3: Phishing message

For ease of remembering, the people have the same password for all their internet accounts. Social engineers usually send an email with link which requires registration and asking to create a username and password. So it is necessary to consider that people always have to create unique passwords for work accounts different from other outside personal accounts and keep changing it often. Phishing attacks are typically executed through the internet which facilitates mass distribution of emails in a short time frame. In recent times, phishing activities have continued to thrive in spite of the technological measures put in place by organizations, campaign by the target industry sectors and the advent of anti-phishing organizations (Odaro and Sanders, 2010). Figure 4 makes unify of human based and computer based social engineering techniques. Besides phishing, it is important to mention the attacks of Reverse social engineering (RSE), Dumpster diving and Shoulder surfing.

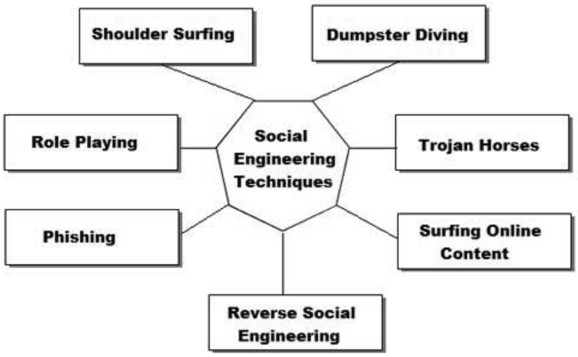


Figure 4: Social engineering techniques

RSE are attacks are especially attractive for online social networks (Facebook, for example). First, from an attacker's point of view, there is a good potential to reach millions of registered users in this new social setting. Second, RSE has the advantage that it can bypass current behavioural and filter-based detection techniques that aim to prevent wide-spread unsolicited contact. Third, if the victim contacts the attacker, less suspicion is raised, and there is a higher probability that a social engineering attack will be successful (Irani, Balduzz, Balzarotti, Kirda, and Pu, n.d.). This form requires the attacker or social engineer to create a person that would seem attractive to the victim and that would encourage the victim to establish contact. Direct asking for passwords or confidential information might raise suspicion, so the social engineer has to stimulate the victim's curiosity and does some form of 'pretexting'. According to Kee (2008:23), Reverse Social Engineering is a more advanced method of social engineering and requires some reconnaissance before a successful attack is employed. Another technique, Dumpster diving is an example where social engineer will prove that someone else's trash is another mans treasure (Kee, 2008:20). Kee points out that, if your trash could be used against you or your company, dispose of properly. Kee (2008:21) also explains the Shoulder surfing. It is when a social engineer watches what you are doing and can also be done remotely (both by cameras and software). For instance, if you happen to be in a computer lab, there will probably be computer cameras around. Those cameras could be public and anyone with an internet connection can logon, zoom in, and see what anyone in the room is doing. Kee stated that, the best thing to do is be aware of your surroundings because you never know who may be watching you.

Wider explanation gives Oosterloo (2008). Oosterloo emphasis that, within the different phases in attack structure several psychological principles and tactics are used to manipulate a person. They are as follows:

- psychological principles:

✓ Strong affect,
✓ Overloading,
✓ Reciprocation,
✓ Deceptive relationships,
✓ Diffusion of responsibility,
✓ Moral duty,
✓ Authority,
✓ Integrity,
✓ Consistency.

- social engineering tactics:

✓ Physical reconnaissance,
✓ People spotting,
✓ Dumpster diving,
✓ Forensic analysis,
✓ Phreaking,
✓ Phishing,
✓ Mail-outs,
✓ Web search,
✓ Profiling,
✓ Physical impersonation,
✓ Virtual impersonation,
✓ Reverse social engineering,
✓ Tailgating,
✓ Piggybacking,

- ✓ Office snooping/Desk sniffing,
- ✓ Item dropping,
- ✓ Data leakage,
- ✓ Direct approach,
- ✓ Identity theft,
- ✓ Malicious software.

COMBATING SOCIAL ENGINEERING

Good security policies and procedures cannot be effective unless they have been consistently applied by the employees. They contain standards and guidelines in order to mitigate the risks of social engineering attacks. Social engineering risk management is a process, influenced by an organizations management and other personnel, applied across the organization, designed to identify social engineering risk and manage this risk to be below the predefined security level, to provide reasonable assurance regarding the achievement of an organizations objectives Oosterloo (2008). Protection against social engineering attacks always starts with education and training. The education and training programs should cover the all safety procedures, policies and methods in order to raise awareness of possible attacks by social engineering. It is very important to secure the confidential information and to have authorization of access to certain classified information. Employees have to know that click on suspicious links might unguarded their log-in credentials and corporation confidential information. More than necessary is to develop a system of periodic inspection of employees and appropriate actions in dealing with social engineering attacks. Basic actions of dealing with the threat of social engineering are password policies and organization of physical security. Password policies include: periodically changing of the passwords; avoiding the possibility of guessing passwords; length and complexity, privacy of passwords and blocking of the account after several attempts. In any organization should be established a system of physical security like identification (ID cars); escort visitors; assessment and organization of security zones with appropriately level of restrictions; engagement of security agencies; as well as respectively destroying of unnecessary documents. All these activities should be uniform and clearly defined, documented in security policies and procedures of the organization and applied by all employees. The employees are responsible for an corporation's integrity and success. Many corporations use a Public Key Infrastructure (PKI) to support confidentiality and integrity to key information. PKI often is used as a mechanism to provide strong authentication of employees as well as access to corporation confidential data.

Public Key Infrastructure-PKI

One of the approaches related to secure information exchange is Public Key Infrastructure (PKI). It is a set of policies, standards and procedures related to authentication, encryption and non-repudiation that all operating within a chain of trust. This subsection describes the elements of PKI, and its advantages. Public Key Infrastructure (PKI) is a popular encryption and authentication approach used by both small businesses and large enterprises (Lawton, 2017). PKI infrastructure is comprised of listed main components: Digital certificates; Public and private keys; Secure sockets layer (SSL) and Certificate Authority (CA). PKI is based on a mechanism called a digital certificate. Digital certificates are sometimes also referred to as X.509 certificates or simply as certificates. Think of a certificate as a virtual ID card (Posey 2005). Posey emphasise that PKI works by assigning a user a pair of keys. These keys are generated by running a mathematical process against the user's certificate. The keys themselves are nothing more than a very long alpha-numeric string. He explains that one of the keys is designated as the user's private key, while the other is designated as the user's public key. The idea is that only the user who owns the keys has the private key, but the user's public key can be freely given to anyone. Normally, a certificate authority or a key management server passes out public keys whenever they are requested, but public keys could really be distributed by any means. According to Lawton (2017), from an operational perspective, PKI is a encryption approach where a pair of cryptographic keys - one public and one private - are used to encrypt and decrypt data. A user can give someone their public key, which that sender uses to encrypt data. The owner then uses their private key to decrypt the data. Posey (2005) gives an example where a user needed to encrypt a file. The explanation is as follows: 'The user would use their private key to encrypt the file. Once the file is encrypted, only the public key can decrypt it. At first, this probably doesn't sound very secure since anyone in the world can have the user's public key just by asking for it. However, there is one detail that you need to consider. The user's public key can only decrypt files, it cannot be used to encrypt anything. Furthermore, it can only decrypt items that have been encrypted using the corresponding private key. Therefore, if a public key is used to decrypt a file, it absolutely guarantees that the person who encrypted it was the owner of the corresponding private key (assuming that the private key hasn't been stolen). For example, if the sender encrypted a file with his private key, and recipient used sender public key to open it, then recipient can be sure that the sender was the person who encrypted the file' (Figure 5).

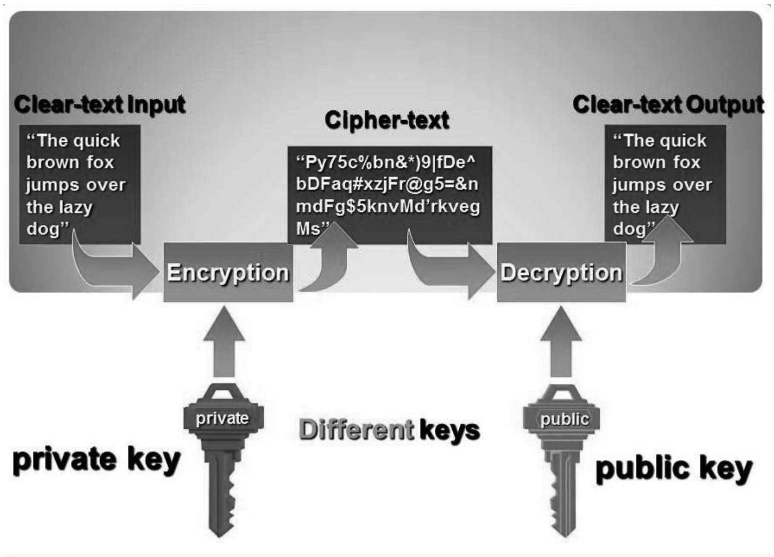

Clear-text Input
"The quick brown fox jumps over the lazy dog"
Cipher-text
"Py75c%bn&*)9|fDe^ bDFaq#xzjFr@g5=&n mdFg$5knvMd'rkveg Ms"
Clear-text Output
"The quick brown fox jumps over the lazy dog"
Encryption
Decryption
private
Different keys
public
private key
public key

Figure 5: Basics of PKI

PKI is asymmetric cryptography technology that enables the creation of verified communication between the public key and the identity of the correspondent private key owner.

Each PKI solution is unique, and supports the distribution, management, expiration, rollover, backup, and revoking public/private keys. Operations supported by the use of public/private key pairs include: Encryption (obscures the contents of files or transmissions to protect against unauthorized viewing); Authentication (verifies the identity of the entity requesting access); Data integrity (reveals any changes to files, programs, transmissions, transmissions, etc .); Nonrepudiation (positive identification between sender and receiver- guarantees that a legal electronic transaction occurred). The owners users of these keys can be people, devices or applications: People (generally use public/private keys for encrypting email messages); Devices (generally use public/private keys for authentication and encryption): Applications (generally use public/private keys for authentication and data integrity) (SANS institute, 2001).

Here is some examples form the article of SANS Institute 'A Business Perspective on PKI: Why Many PKI Implementations Fail, and Success Factors To Consider':

Encryption example: The most common use of public/private keys is for encrypting email messages between people. If Ann wants to encrypt a message for Clark:

- Clark would make his public key available (as an attachment to an email sent to Ann, through a directory or a public key exchange site accessible to both Ann and Clark, etc.).
- Ann would compose and address the email message and signal the email software to encrypt the message (usually by clicking on a icon or selecting the action from the Toolbar).
- The email software would use Clark's public encryption key, which is stored with his information in Ann's email address book or available in a shared area, to encrypt the message.
- Ann sends the encrypted message to Clark.
- Clark's email software receives the message and automatically tries to decrypt it using Clark's private encryption key, or through a dialog box, offers to decrypt the message.
- If the email message was really encrypted using Clark's public key, then Clark's private key will decrypt the message so Clark can read it.

Another example illustrates how the use of public/private keys can provide authentication and indicate whether information has been tampered with or corrupted during transmission.

Authentication and Data Integrity example: Signing a message involves using a private key instead of a public key of the intended key recipient. Signing provides both authentication and data integrity. Again using the example of sending a message between two people Ann and Clark:

- Ann composes a message for Clark, and signs it by clicking on the icon on the Toolbar.

• The email software accesses Ann's private signature key and runs a calculation on the message and any attachments, producing a fixed-length number called a hash which is a unique representation of the contents. This number is sent along with the message to Clark.

• When Clark receives the message in his email software, Ann's public signing key is located and used to run the same calculation on the message and attachments.

• If the hashes match, Clark has proof that

✓ the message really came from Ann, and

✓ nothing in the message was changed from the time that Ann signed and sent it only because its public keying key could produce the same hash value.

In the article of cryptography part 5 'The Mathematical Algorithms of Asymmetric Cryptography and an Introduction to Public Key Infrastructure', available on the INFOSEC INSTITUTE web site, are explained the basic premises of PKI. It is clearly noted that the PKI is to help create, organize, store, and distribute as well as maintain the public keys. In PKI infrastructure, both of the public and private Keys are referred to as 'digital signature'. They are created by a separate entity known as the 'Certificate Authority' (CA), not by the sending and the receiving parties. The digital certificate consists of both the public key and the private key, issued by the relevant CA. This is also the entity that verified digital certificate. The digital certificates are typically kept in the corporation's central server. The databases that collect and distribute the digital certificates from the CA are the LDAP or X.500 directories. Another term is the Registration Authority (RA) that usually exists in big multinational corporation. RA handles and processes the requests for the required digital certificates and then transmits those requests to the CA where are created the required digital certificates. To summarize, the Public Key Infrastructure (PKI), as a specialized form of asymmetric cryptography, offers a higher level of security not only by using the public key/private key combination but also by making use of the CA. CA is trusted, third party governing body of PKI, where all public key/private keys are created and verified. This is important to ensure the integrity amongst the digital certificates, related to the communication process for both, the sending and the receiving parties. Another mechanism of security is RA which confirms the identities of the sending and receiving parties that are requesting the public key/private key combinations. The parties must be uniquely identifiable within each CA and the verification process provides that information (Figure 6).

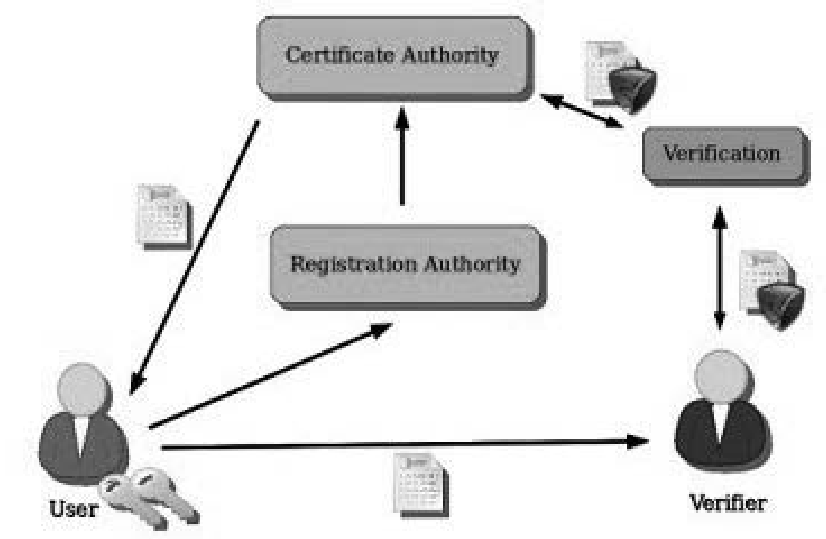


Figure 6: Public key infrastructure

Mentioned, related to function and operation of CA and RA is tightly connected with various policies and rules. According to INFOSEC INSTITUTE article 'The Public Key Infrastructure Policies and Rules' the following is just a sampling of some of the points which need to be addressed when a Public Key Infrastructure is deployed:

- Where and how the records and the audit logs of the Certificate Authority are to be kept, stored, and archived.
- The administrative roles for the Certificate Authority.
- Where and how the public keys are the private keys are to be kept, stored, and also backed up.
- What the length of time is for how long the public keys and the private keys will be stored.
- If public key or private key recovery will be allowed by the Certificate Authority.

- The length of the time of the validity period for both the public keys and the private keys.
- The technique in which the Certificate Authority can delegate the responsibilities to the Registered Authority.
- If the digital certificates which are to be issued by the Certificate Authority are to be delivered.
- If the digital certificates to be issued by the Certificate Authority are to be used for the sole purpose of just encryption of the Ciphertext.
- If there are any types of applications that should be refused to have digital certificates.
- When a digital certificate is initially authorized by the Certificate Authority if there will be a finite period when the digital certificate will be subject to revocation.

Besides education, strong password polices and as well as installing updates to the corporation computer system is important to ensure that devices only communicate with other trusted devices. Attacks against corporation computer infrastructure have existed as long as technologies development. Also, with the globalization, increases the numbers of corporations in all parts of the world significantly changed corporative acting and the threats manifestation and perception.

Maintaining the trust is an integral component for implementing a PKI. To facilitate trust PKI must be managed with policies, standards and procedures. Through a risk assessment, it is possible to reduce the attacks and implementation of required PKI policies, standards and procedures makes the compromise much more difficult.

Brown (2001) explains the PKI 'Questions of trust'. Brown states that besides being a technology based on public/private keys and digital certificates, PKI is also a trust network which operates at several levels. They are:

- trust between organizations and their PKI service providers (Certificate Authorities for example),
- between companies and their trading partners, and
- among individual employees.

According to Brown (2001), the basis, of an employee education program in support of a successful PKI program, is the fundamental security concepts presented in Table 1.

Concept	Meaning	Traditional Method	PKI Mechanism
Privacy, Confidentiality	Information is available only to those authorized for it.	Sealed envelope Invisible ink message.	Encryption with a public key ensures that only the owner of the paired private key can decrypt the message.
Authentication, Identification	You are who you say you are and you have rights to entry or information	Employee ID, driver's license, passport Mother's maiden name	A digital certificate issued by a trusted certificate authority binds a public key to an individual
Integrity	Information is genuine and unaltered.	Permanent ink Letterhead stationary, water-marked paper	A digital signature comprising a message digest and the sender's private key can be validated using the sender's public key.
Non-repudiation	Evidence that an activity or transaction cannot later be denied.	Notarized signature, Paper trail Registered mail	The digital signature validating a transaction can only be created by the private key holder

Table 1: Fundamental Security Concepts Embodied by PKI

The purpose of a PKI is to manage keys and certificates by establishing and maintaining a trustworthy corporation networking environment. In other words, PKI facilitate the secure electronic transfer of information and enables the use of encryption and digital signature services across a wide variety of applications. As a high level of access to a corporation computer infrastructure, PKI is a target for social engineers. By compromising a PKI, social engineer makes further his attack more effectively. So, it is necessary to develop a strong process that ensures that the PKI is run with oversight from the proper teams within corporations.

CONCLUSION

Due to the increasing influence of social engineering to cooperative security, it may be only a matter of time until a social engineer targets an employees at your corporation. No matter in what form social engineering appears (human or computer based), deception takes advantage of the human naivety. Attacker, defender, and the victim are in the circle of deception in which each has its own role of acting. Internet has possibility to facilitate mass distribution of emails and the social engineers widely use that, so it is important to understand what indicates that is a fraud. On the other hand, an understanding of how to identify a social engineering attack cannot guarantee the corporation complete protection. The process should focus on several layers in the corporation. With proper education and training, the employees could be one of the best defenders against social engineering manipulations and fraud. Education, training and control activities are policies and procedures witch support the measures against social engineering. PKI is the solution of combating social engineering. As a set of policies, standards and procedures PKI is a popular encryption and authentication approach used by corporations. Depending of corporation's security requirements deployment and establishment of a Public Key Infrastructure should be quite complex, led by many rules and policies established within the corporation. Encryption and digital signature services, across a wide variety of applications, support confidentiality and integrity of corporation key information. PKI is a encryption approach and provides strong authentication as well as access to corporation confidential data. Trust is an integral component for implementing a PKI. Confidentiality, authentication, integrity and non-repudiation, as a fundamental security concepts embodied by PKI, maintain a trustworthy corporation networking environment.

REFERENCES

Oosterloo, B. (2008) *Managing Social Engineering Risk: Making social engineering transparent*, Master thesis Industrial Engineering and Management, University of Twente: Enschede, The Netherlands.

http://essay.utwente.nl/59233/1/scriptie_B_Oosterloo.pdf

Gulati, R. (2003) 'The Threat of Social Engineering and Your Defense Against It', SANS Institute InfoSec Reading Room, pp 1-12.

https://www.sans.org/reading-room/whitepapers/engineering/threat-social-engineering-defense-1232

Cortez, P. (2013) 'Human based social engineering in the workplace', Tech First Magazines 2013.

https://www.technologyfirst.org/magazines/2013/51-april/839-pete-cortez-technical-instructor-new-horizons-computer-learning-centers.html

Ablon, L. (2015) 'Social Engineering Explained: The Human Element in Cyber Attacks', The Cipher Brief, October 19, 2015.

https://www.thecipherbrief.com/article/social-engineering

Evans, J. N. (2009) 'Information technology social engineering: an academic definition and study of social engineering - Analyzing the human firewall', Graduate Theses and Dissertations, Iowa State University.

http://lib.dr.iastate.edu/cgi/viewcontent.cgi?article=1701&context=etd

Kohlberg, M. and Kowalski S. (2008) 'The Cycle of Deception – A Model of Social Engineering Attacks, Defences and Victims', Proceedings of the Second International Symposium on Human Aspects of Information Security & Assurance (HAISHA 2008).

Malcolm, A. (2007) 'Social Engineering: A Means To Violate A Computer System', SANS Institute InfoSec Reading Room, pp 1-13.

https://www.sans.org/reading-room/whitepapers/engineering/social-engineering-means-violate-computer-system-529

Odaro, S. U. and Sanders, G. B (2010) 'Social Engineering: Phishing for a Solution', Centre for Security, Communications & Network Research University of Plymouth, U.K.

Irani, D., Balduzzi, M., Balzarotti, D., Kirda, E., and Pu, C. (n.d.) 'Reverse Social Engineering Attacks in Online Social Networks'.

http://s3.eurecom.fr/docs/dimva11_reverse.pdf

Kee, J. (2008) 'Social Engineering: Manipulating the Source', SANS Institute InfoSec Reading Room, pp 1-31.

https://www.sans.org/reading-room/whitepapers/engineering/social-engineering-manipulating-source-32914

Lawton, S. (2015) 'Introduction To Public Key Infrastructure (PKI)', in tom'sIT PRO real-world business technology, MARCH 17, 2015.

http://www.tomsitpro.com/articles/public-key-infrastructure-introduction,2-884.html

Posey, B. (2005) 'A beginner's guide to Public Key Infrastructure', in TechRepublic, September 15, 2005.

https://www.techrepublic.com/article/a-beginners-guide-to-public-key-infrastructure/

SANS institute (2001) 'A Business Perspective on PKI: Why Many PKI Implementations Fail, and Success Factors To Consider',SANS Institute InfoSec Reading Room, pp 1-9. https://www.sans.org/reading-room/whitepapers/vpns/business-perspective-pki-pki-implementations-fail-success-factors-728

'The Mathematical Algorithms of Asymmetric Cryptography and an Introduction to Public Key Infrastructure', INFOSEC INSTITUTE.

http://resources.infosecinstitute.com/mathematical-algorithms-asymmetric-cryptography-introduction-public-key-infrastructure/#article

'The Public Key Infrastructure Policies and Rules', INFOSEC INSTITUTE, Posted in Public Key Infrastructure (PKI) on February 13, 2017.

http://resources.infosecinstitute.com/inner-components-policiesrules-public-key-infrastructure/#gref

Brown, K.J. (2001) 'PKI and Information Security Awareness: Opportunity and Obligation', SANS Institute InfoSec Reading Room.

https://www.sans.org/reading-room/whitepapers/vpns/pki-information-security-awareness-opportunity-obligation-750

UDC 005.334

PROVIDING CORPORATE SECURITY IN CRITICAL INFRASTRUCTURE PROTECTION PROCESSES – RISK OF OUTSOURCING

Miran Vršec, MSc, Denis Čaleta, PhD
Institute for Corporative Security Studies, Ljubljana

This paper discusses risk management in terms of importance, role and risks of outsourcing integrated into the processes of providing corporate security in entities that are part of critical infrastructure. Taking into consideration that every individual country is only part of the global market, outsourcing needs to be considered in a wider context, i.e. from a global perspective and together with the related impacts. The reason for it is that outsourcing entities, too, are increasingly operating on a global scale. Therefore, it is crucial that a wider global perspective is adapted in discussions. In the context of growing globalization resulting in the networking and integration of business, cultural and other entities coming from different geographic and cultural environments, the opening of the labour market and the related free movement of workers, new risks have emerged which can significantly change the view on outsourcing and its role in the processes of providing corporate security, the mission of which is the provision of safe and smooth operation of business and other processes in business and other critical infrastructure entities in everyday situations, and especially in crisis situation (natural disasters, major accidents at work and environmental disasters, epidemics, terrorist acts, organized international crime etc). Obviously, outsourcing is paid far too little or even no attention in building comprehensive integrated security systems, which may have a critical (negative) impact on risk management and may lead to unexpected loss events and failure of individual processes or entire systems, despite systematic security solutions of great quality. The purpose of this paper is to show the significance and role of outsourcing in providing corporate security both at the operational and the strategic levels, as well as to present the risks related to the integration of outsourcing into the processes of providing corporate security.

INTRODUCTION

In the operation of their organizations (business entities), the owners and management strive towards their primary objective, i.e. the achievement of the highest possible added value, the maximization of the profit in the longest possible run and the increase in the value of the company as such. Trying to meet these objectives, they also increasingly use different modern management tools and introduce good practices in order to achieve an optimal use of resources and available time and thus achieve maximum effects of business processes and organization as a whole. It is basically the fulfillment of the general "minimax" economic principle, i.e. to achieve the maximum output for the minimum input.

Businesses that are a part of critical infrastructure of a certain country, and thus of a certain region, have to be primarily considered in relation to the ownership structure of the businesses and activities (sector) in which the entity operates. These business entities are usually large, and characterized by joined ownership, whereby the minority or majority ownership is directly or indirectly associated with the state. The smooth operation of the entities concerned is essential for the smooth operation of vital activities of the state as a whole. For these entities, the above-mentioned "minimax" principle is less significant. Considering the introduction of integrated security solutions at corporative level and building a corporate security system through which critical infrastructure entities ensure smooth functioning and business operation, the above-mentioned fundamental "minimax" economic principle is of secondary importance. When building a comprehensive system for the management of business security risks at the strategic level, the minimum input and maximum output should no longer be the issue. Instead, we should focus on the necessary input and the optimal output which ensure a timely detection and elimination of hazards, an effective warning and response system, and prompt and effective elimination of potential consequences of an incident. An important segment in developing the above mentioned philosophy of thinking and operation is also represented by all outsourced entities providing different contract services and activities for the critical infrastructure entities that may be of key (strategic) importance for the operation of these critical infrastructure entities. In this regard, outsourcing can be essential for the functioning of business entities, and the introduction of outsourcing can be a crucial strategic decision for the owners and management (for more details, see Greaver, 1999).

We can therefore conclude that people with their skills, knowledge and appropriate motivation are one of the key factors in ensuring the reliability of outsourcing. This conclusion is important also from the security point of view, for people play a key role in the corporate security system.

STARTING POINTS ON OUTSOURCING

In the past, owners and management shared a general belief that the effectiveness of an organization can be increased solely through the increase in the effectiveness of individual business processes within individual business functions and within the organization as a whole.

Therefore, all endeavors were oriented towards the search of internal reserves and optimal combinations of available resources. When this could no longer suffice, organizations realized it was necessary to search for new markets, in particular outside the borders of home country, which resulted in the formation of first international connections that lead to ever growing globalization of the market and operation of organizations. Rapid growth caused more and more problems to organizations. Becoming larger, they were also becoming less flexible and slower to adapt. What is more, they were becoming less cost- effective. Ideas started to emerge on the transfer of particular segments of activities to contractors who specialized in particular activities and were highly flexible and far more cost-effective. Outsourcing was becoming a special purchasing strategy and an increasingly important strategic decision of organizations. Today, the greatest challenge for companies is the question of how to adapt as quickly as possible to changes on global and local markets and how to remain competitive in the long-run. Certainly, outsourcing makes it easier, since companies can, in a more thorough and effective manner, focus on the development of their core activity.

However, in doing so, they should not neglect the fact that outsourcing brings not only benefits, but also some risks, which are to be discussed below.

Definition of outsourcing

The concept of *outsourcing* derives from the word phrase »outside resource using« and refers to the use or rental of external resources for the need of the operation of one's own organization. An organization entrusts particular activities or entire business functions to outside contractors that could also be provided in-house, while more or less keeping its core competencies. Individual authors, of course, offer different definitions of this concept. Their definitions mostly depend on the type of activity and their scope. What is more of less common to all of them is that it is a transfer or an award of a contract for one or several internal activities to another organization, which thus becomes an external contractor.

Why should outsourcing be introduced

Outsourcing is a means or tool for the management to successfully achieve strategic business guidelines and goals of its organization, primarily associated with an increase in efficiency, adaptability to changing conditions in the internal and external environment and reduction of its operating costs. Outsourcing is primarily used for the purpose of the management and reduction of costs of the organization, which is too often the sole purpose of an organization. In this way, different investments can be avoided in the short run (e.g. equipment acquisition, facility expansion). Instead, an organization can use its resources for the development of its core competencies, key personnel and for new knowledge acquisition. Of course, it needs to be assessed whether short-run benefits of outsourcing can also be felt in the long run, and what is the long-term influence on the long-term development and growth of the organization. Furthermore, it has to be taken into consideration that an organization should never allow itself to be entirely dependent on outsourcing, for this could present too great a risk for the organization in the long run (Power/Desouza/Bonifazi, 2006). Along with the development of outsourcing, activities have expanded which have become the subject of outsourcing. Recently, it can be observed that organizations have also outsourced some significant support or even core processes or activities, such as: legal affairs, accounting services, IT, parts of production processes, logistics (transport services and storage) as well as certain parts of personnel function. This makes an organization more open and flexible, but also more vulnerable. In terms of security, this presents higher and higher risks that need to be systematically managed.

The literature overview (e.g.: Stees; Greaver, 1999; Kehal and Singh, 2006; Power/Desouza/Bonifazi, 2006; Oshri/Kotlarsky/Willcocks, 2009; Stanger, 2011) shows that an increased emphasis has been given to the consideration of benefits that come with outsourcing, such as: cost management and reduction, influence on the reduction of investment needs, conversion of fixed costs into variable costs, higher level of quality and reliability of operation, increase in flexibility and adaptability, orientation towards the development of organization's core competencies and focus on key customers. However, many experts have recently warned about the dangers of outsourcing, e.g. smaller savings than planned, poor quality of performance, hidden costs, wrong selection of outsourcing partner, loss of expert knowledge, business partner take-over, loss of the key employees and loss of contact with key customers.

It should be pointed out that these dangers usually pertain to companies associated with early termination of outsourcing contracts and transfer of performance of operations to activities in the processes, while there is too little discussion about long-term strategic aspects and guidelines for outsourcing, both in terms of benefits and risks, including those with a direct influence on security situation in an organization. Much too often, outsourcing is considered solely in terms of the transfer of activities to outside contractors, while no consideration is given to the necessary integration of outsourcing into the organization's support processes.

INTRODUCTION OF QUALITY OUTSOURCING INTO THE CRITICAL INFRASTRUCTURE MANAGEMENT SYSTEM

Definition of critical infrastructure

In 2005, the European Commission adopted the Critical Infrastructure Protection Program (Green Paper on a European Program for Critical Infrastructure Protection, COM (2005) 576 final, Brussels, 17 November 2005). Its

Annex (Annex 2 – Indicative List of Critical Infrastructure Sectors) provides an indicative list of economic and state sectors managing critical infrastructure, namely: (1) Energetics, (2) Telecommunications, information technology, postal service, (3) Water, (4) Food, (5) Health, (6) Banking, finance, (7) Public authorities, (8) Civil institutions, (9) Transport, (10) Chemical and nuclear industry, (11) Research and creations.

According to the Council Directive (EU) No. 114/2008 of 8 December 2008 on the identification and designation of European critical infrastructure and the assessment of the need to improve their protection that followed the above-mentioned program, only energetics and transport are classified as cross-sectors of European critical infrastructure that operate in two, three or more countries.

Pursuant to the Directive, each EU member state shall identify which sectors to include in the national critical infrastructure.

Critical infrastructure protection and the protection of citizens are becoming reality and one of the most important segments of the European security policy and European security system in the EU and individual EU member states. The EU and its member states have demonstrated vulnerability. Obviously, terrorism, more than all other incidents, initiated certain activities of European institutions (European Commission and others) which have started to work on specific projects to raise the level of security control in the European area. Concerning vulnerability, threats and security risks in the EU as well as protection of vital facilities, i.e. critical infrastructure (for more see Lewis, 2006; Murray, 2007; Biringer/Metalucci/Conor, 2007), it is nevertheless important to realize that threats are not posed only by terrorism (for more see Prezelj, 2008; Čaleta, 2014) but also take various other forms which are a cruel present and future reality. These forms are natural hazards, climate change, environmental incidents, industrial accidents and crime-related threats. These are all long-term, multifaceted and complex threats that have to be addressed in terms of damage and loss prevention, and in terms of civil and professional response to incidents.

Security mechanisms for the management of risks in outsourcing

When considering the security related to the outsourcing service provider, the following questions will arise:

- Who will directly perform outsourcing services?
- How is the outsourcing personnel security cleared and what social and cultural groups do they come from?
- What security system is established by the outsourcing service provider?
- What are long-term cooperation opportunities?

The above and several other questions should be considered by both the contracting entity as well as the outsourcing service provider. Outsourcing is a marathon rather than a sprint, and it involves several intermediate stages. It is a long-term partnership, whereby outsourcing and its service become an integral and indispensable part of business processes and operation of an organization. As a rule, organization's success also depends on the quality of this partnership.

The outsourcing provider has to be particularly aware of the fact that service performance for the needs of critical infrastructure entities requires significantly more engagement of security mechanisms in managing business security risks emerging in the business process and environment of the outsourcing provider.

In the initial phase, the outsourcing provider has to elaborate vulnerability, threat and business-related security risk assessment, on the basis of which it can identify and analyse vulnerability, the level of threat and business security risks, and develop appropriate security measures and solutions to deal with these problems in a comprehensive manner. Efforts should be clearly focused on the development of integrated security system which ensures a comprehensive management of business security risks, both at the strategic and operational levels. In this manner, the outsourcing provider actually manages risks in all business functions and process phases.

One of the main integrated security system elements is control, by means of which we constantly check the adequacy and effectiveness of risk management mechanisms at various operating levels. With the introduction of improvements, the control enables the smooth operation of the security system in the long-run.

However, taking all this into account, the essence of cooperation between business entities – mutual trust and understanding – should not be disregarded. This is essential, no matter how good the security mechanisms might be. Along with legal and operational definitions, such partnership largely depends on business ethics and ethics of the relationship as such.

Subject of the contract with the selected outsourcing provider

After the selection of the outsourcing provider, the subject of the contract should be negotiated. Since the partners are mutually dependent, this phase is based on complete trust between both partners. Thus, a contract should not be signed in a »win-lose« manner. Rather, a contract should be developed in such a way as to enable the resolution of potential disputes. It has to be complex depending on the complexity of the outsourced service. For complex projects, contracts can be drawn up in two parts. The general part defines the legal frameworks, while the second part details the rights and obligations of both partners (Bongard, 1994). When drawing up a contract, the contract should also include the benefits for the contractor, following the "win-win" model.

In line with good practices, the contract should contain 7 sections (Bongard, 1994), namely:

1. **Task specification –** partners specify the types of work for transfer, the duration of the contact and the period of work performance,
2. **Required level of service** – the required service delivery standards must be set for all the works. The standards must be measurable.
3. **The rights and obligations of both partners** – the contract should specifically define the rights and obligations of each contracting party.
4. **Transitional period** – an important aspect of the external process and concerns, inter alia, the transfer of personnel, training of outsourcing employees, transfer of means of production, and monitoring the performance of activities.
5. **Price, terms of payment and contract duration.**
6. **Contracting management** – the time schedule of reporting and the method of solving problems related to non-compliance with contractual provisions.
7. **Specific clauses** – liquidated damages, introduction of standards and business tools etc.

When signing contracts with outsourcing providers, critical infrastructure entities also need to define outsourcing commitments on the provision of risk management system within their organizations. This means that in the contract, the outsourcing providers commit to the manner of:

- managing business security risks in their organization and working environment,
- applying occupational health and safety security measures on the location of performance of contract works,
- performing fire safety measures on the location of performance of contract works,
- providing appropriate personnel that is to perform the contract works,
- protecting personal and confidential data and business secrets they can access during the performance of contract works,
- monitoring the contract work performance,
- managing security mechanisms in their organization and ensuring their proper functioning.

Given the complexity of the contents of this part of the contract resulting from the critical infrastructure entity security needs, the contents concerned can be defined in a special act which is attached to the contract and its integral and inseparable part.

The quality of contract relationship is primarily influenced by the following 10 success factors (Source: Outsourcing Consortium, www.outsourcing.com):

- Understanding company goals and objectives
- Strategic vision and plan
- Selection the right contractor
- Ongoing management of the relationships
- Proper structure of the contract
- Open communication with affected individuals/groups
- Support and involvement of senior executives
- Careful attention to personnel issues
- Short-term financial justification
- Use of external expert opinion

Past experience with tragic events (e.g. terrorist attacks in the U.S.A., Great Britain, Spain, Africa and elsewhere) show that the area of human resources represents the greatest risks.

Perpetrators of terrorist and other criminal acts use outsourcing as a springboard for the performance of their acts.

They use outsourcing to infiltrate into an organization and secretly prepare the environment for the performance of their criminal acts (gathering information, identifying process and loopholes, searching for loopholes in the security system, and searching for potential partners for performing criminal acts, etc.). Personnel-related risks are difficult to recognize and manage. Therefore, greater attention should be paid to them.

Deliberate introduction of outsourcing into the system and process of critical infrastructure management

The majority of critical infrastructure assets in Slovenia are owned by the state.

This means that most services are outsourced through the public procurement system, whereby the lowest bidder is selected. Thus, the main criterion is the price rather than the quality. Naturally, good quality is expected. But how can the lowest price (which often does not even cover the costs) ensure the expected quality or the quality compliant with ISO 9001:2008 standards, safety standards and corporate social responsibility?

The following activities or parts of processes involve risk when fully outsourced:

- IT management,
- Accounting,
- Personal and confidential data management,
- Business secret management.

The appropriate selection of outsourcing provider is therefore crucial for the successful process of introducing outsourcing into the organization of critical infrastructure entity.

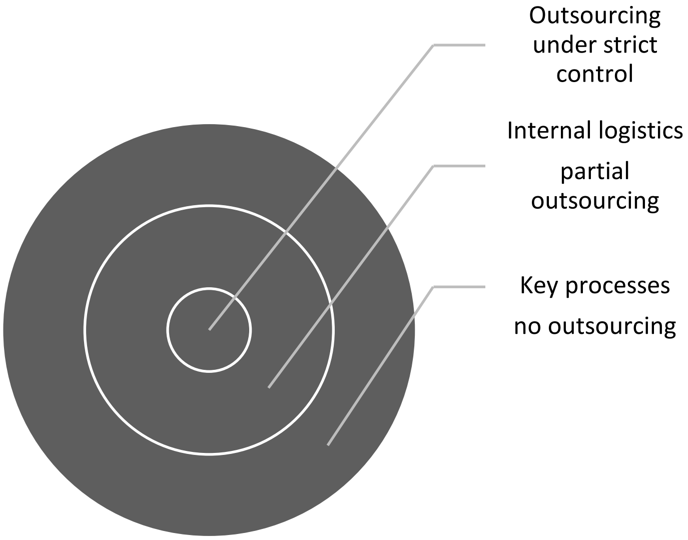

Outsourcing under strict control
Internal logistics partial outsourcing
Key processes no outsourcing

Figure 1: Introduction of outsourcing into the critical infrastructure management systems and processes

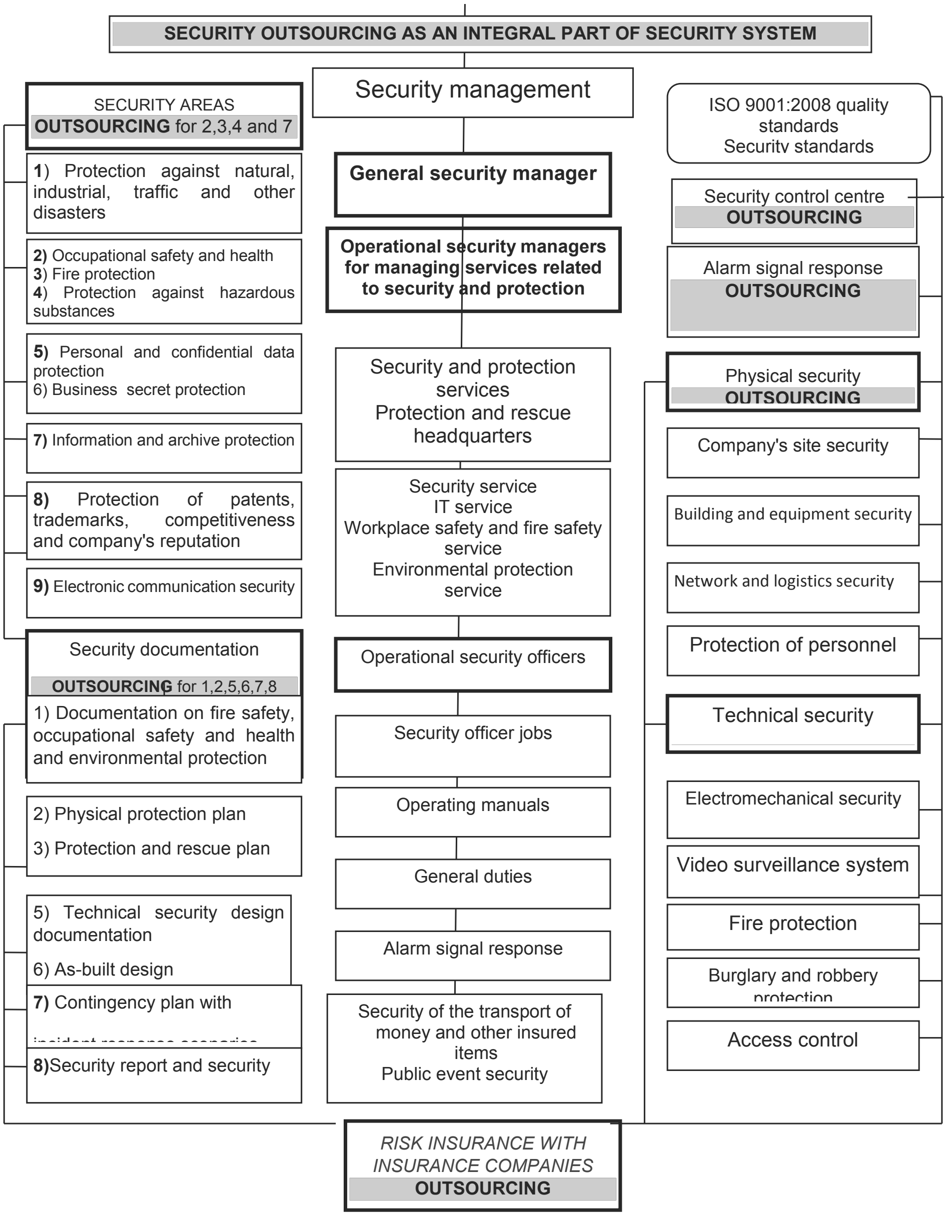
As mentioned above, the outsourcing provider is usually selected through the public procurement system. Therefore, the preparation of appropriate documentation related to the call of tenders is essential. The documentation has to include at least all the references referred to in this paper. The preparation of bidding documents is a complex and broad topic. It goes beyond this paper, and should be explored in some other paper.

THE ROLE OF OUTSOURCING IN INTEGRATED SECURITY SYSTEMS IN COMPANIES AND OTHER ORGANIZATIONS

Security of an organization is no longer a side issue. It has become an integral part of its policy, strategy, economics, business dynamics, culture, reputation, development, growth and collapse. This means that the level of security selected by the owners, management, supervisors and employees when trying to achieve positive business results is of great importance. Loss and damage event prevention is becoming crucial, and so is the belief that the security mechanisms are the elements used for professional management of vulnerability, threats and risks. Thus, security activities have been recognized as an important factor of work and business efficiency and performance, and hence one of the factors for increasing competitiveness (competitive advantage) of every organization, which is the condition for its survival in modern and crisis market conditions.

It is obvious that the new thinking related to the security of companies rests more on economic, business and ethical values and standards that apply in economy, and less on the state and its repressive institutions. The organization must be the first to respond when its assets, capital, profits, employees, intellectual and industrial property, business secret, competitive advantage, reputation and other values are under threat. Timely and professional response requires knowledge on security, warning and protective mechanisms within an organization, as well as knowledge and information about the control system and its external dangers and threats. It is also good to know what can and should be done – in cases of deviance in the economy – by state institutions in the discharge of their official duties, what is the role of the audit and inspection system, and where the company can order high-quality physical, technical, advisory, educational and other security services. The main issue is how to build a modern, economical, professional and independent security system in an organization, which is based on the principle of optimal protection and which ensures an appropriate level of security, cost management and protection benefits (cost/benefit) and loss prevention. It concerns the establishment of an integrated security system with integrated security which consists of interconnected and interdependent areas of expertise related to security, such as: protection against natural and other disasters, occupational health and safety, fire protection, environmental protection, data protection, protection of information and business secrets, physical and technical security, civil protection, etc. The conditions for introducing integrated security are the following: compliance with regulatory requirements, introduction of security standards, quality assessment of security solutions within the quality system management, and the improvement of the level of safety culture of employees and business ethics of the management.

Discussions on organization's security issues and the role of the state, audit, private security sector and others have become topical and taken place within parliamentary systems, entrepreneurship, supervising institutions and the mass media. This is further reinforced by crisis management situations which require a professional handling of security issues of companies and economy as a whole (Borodzicz, 2005; Vršec, 2011). Negligent security in organizations can be fatal. This fatality may lead to notorious and far-reach-


SECURITY OUTSOURCING AS AN INTEGRAL PART OF SECURITY SYSTEM
Security management
SECURITY AREAS
OUTSOURCING for 2,3,4 and 7
1) Protection against natural, industrial, traffic and other disasters
2) Occupational safety and health
3) Fire protection
4) Protection against hazardous substances
5) Personal and confidential data protection
6) Business secret protection
7) Information and archive protection
8) Protection of patents, trademarks, competitiveness and company's reputation
9) Electronic communication security
Security documentation
OUTSOURCING for 1,2,5,6,7,8
1) Documentation on fire safety, occupational safety and health and environmental protection
2) Physical protection plan
3) Protection and rescue plan
5) Technical security design documentation
6) As-built design
7) Contingency plan with
8)Security report and security
General security manager
Operational security managers for managing services related to security and protection
Security and protection services
Protection and rescue headquarters
Security service
IT service
Workplace safety and fire safety service
Environmental protection service
Operational security officers
Security officer jobs
Operating manuals
General duties
Alarm signal response
Security of the transport of money and other insured items
Public event security
ISO 9001:2008 quality standards
Securitv standards
Security control centre
OUTSOURCING
Alarm signal response
OUTSOURCING
Physical security
OUTSOURCING
Company's site security
Building and equipment security
Network and logistics security
Protection of personnel
Technical security
Electromechanical security
Video surveillance system
Fire protection
Burglary and robbery protection
Access control
RISK INSURANCE WITH INSURANCE COMPANIES
OUTSOURCING

ing economic, financial, business and other scandals, huge financial loss, ethical damage, economic crime and numerous audit requests in order to determine the constitutionality, legality and ethics of the ownership, organizational, financial and personnel transformation, looking for possible fraud and error. In this respect, mechanisms for the prevention and management of all possible hazards to work, business and management of organizations should be perceived as positive. Anything that brings financial, business and moral damage is detrimental to an organization. The sum of all damages and losses in a particular organization can be devastating and frightening, often leading to entropy and collapse. Thus, most organizations face all-encompassing internal and external treats and crisis in the transformation process.

It is the commercial, social and business – i.e. economic – security of organizations that is threatened.

Taking into account the conditions and circumstances of organizations' crisis management and leaving most safety concerns to organizations themselves, (particularly) the actual owners, management teams and security experts will have to make many complex organizational, technical, information, educational and other interventions to establish their own warning, surveillance and protective mechanisms.

Only an organization with modern security and control mechanisms can be sound, internally solid, successful, competitive and enjoying high reputation. The umbrella management and security management should go hand in hand to define **what the organization will protect by itself and what can be outsourced** to achieve this objective (Vršec, 2009). An organization designed in this manner has a high chance of fast breaking into the European and global market and business scene. Indeed, quality in-house security and security outsourcing are no doubt a competitive advantage. Next pages discuss an integrated security system (Table 1) in which quality security outsourcing can be introduced.

Most security outsourcing pertains to physical and technical security and the management of security control centers, and in that regard also to alarm signal response. This is followed by outsourcing of fire protection services, occupational safety and health and information security. A special outsourcing area refers to the insurance of various risks at insurance companies, enabling the creation of financially attractive insurance portfolios.

THE MANAGEMENT OF OUTSOURCING RISKS IN CORPORATE SECURITY MANAGEMENT PROCESSES

In corporate management theory and practice, risk taking is a normal, logical and essential phenomenon in every corporation, affiliated group, business system and individual company. In this context, risk avoidance means that an organization's management is incompetent, ignorant and unwilling to confront challenges, danger, changes, business opportunities and development strategy which involves many risks. An interesting idea on risk taking in the decision process was developed by the former U.S. Secretary of State Colin Powell, who recommends a 40/70 formula and advises: "*Don't take action if you have only enough information to give you less than a 40 percent chance of being right, but, don't wait until you have enough facts to be 100 percent sure, because by then, it is almost always too late.*

Once the information is in the 40 to 70 range, go with your gut" (in Berk, 2005, p. 21; similarly Broder, 2006).

Due to many changes of internal and external origin and conscious risk-taking, companies incorporate risk management into their business policy, development strategy, decision-making processes and relationships with business partners and outsourcing in order to prevent or minimize the economic, material, financial, human and moral damage and loss.

It is an extremely important business security philosophy of those owners, operators, management and supervisors who bring **incident, damage and loss prevention** in business process management to the fore. **The same philosophy is adapted by the owners and outsourcing management** who produce particular products for or provide services to contracting authorities. Business results and profits of contracting authorities also depend on costs, quality and risks related to outsourcing.

Contracting authorities – corporations, affiliated groups, companies, public corporations, institutes, state institutions and other organizations – have to be aware that the introduction of outsourcing involves certain risk in terms of costs, quality, reliability, security, long-term operation and operation in crisis situations.

In this perspective, the following outsourcing risks should be recognized:

- Inadequately educated, unprofessional, uncommunicative or chaotic or crime-prone management,
- Intransparent or low-quality performance of contractual obligations,
- Poor internal control,
- Low motivation of workers due to low salaries and poor labour relations,
- Poor working conditions and low level of occupational health and safety,
- Removal of confidential data, information and documentation,
- Low level of responsibility,
- No security standards,
- People working at workplaces exposed to risk and with knowledge of confidential information have not been security-cleared,
- Non-compliance with security measures in the area of and at the facilities of contracting authority,
- Poor business results – insolvency and illiquidity,
- Slow response to changes and additional requests of contracting authorities,
- Ignoring of contracting authority's warnings about mistakes,
- No guarantee about the contractor's business continuity in the event of trouble or crisis,
- No priorities determined regarding the fulfillment of contractual obligations to different contracting authorities in an emergency response requiring multiple response, etc.

The above-mentioned and other outsourcing risks are an integral part of risks related to business, finance, information, communication, market, logistics and security. This fact is disregarded by many contracting authorities who are surprised to encounter problems in their outsourcing process. In order to avoid such surprise, the questions indicated above, which are related to the above-mentioned risks should be addressed prior to the selection of the best outsourcing provider. Therefore, the quality of products and services, and the reputation of contracting entity depend on the organization of outsourcing. Outsourcing risk management falls within the corporate management framework, where the project of risk management is also given priority.

Table 2: Universal risk management model (adapted from: Universal Business Risk Model of the global consulting firm Arthur Andersen)

<table>
<tr><td>Environment risk Political risk Access to capital</td><td>Customer Industry</td><td>Technological innovations Shareholder's relations</td><td>Sensitivity Directives Standards</td><td>Legislation Competition</td><td>Disasters Financial markets</td></tr>
<tr><td colspan="2">**Operational risk –Process risk**</td><td colspan="2">**Risks related to the delegation of authority**</td><td colspan="2">**Financial risks**</td></tr>
<tr><td colspan="2">• Customer's satisfaction
• Human resources
• Intellectual capital
• New product development
• Operating efficiency
• Capabilities span
• Production time
• Availability of resources
• Marketing channel
• Partner links
• Regulatory compliance
• Business interruption
• Product/services defect
• Pollution
• Occupational safety and health
• Damage to reputation and goodwill</td><td colspan="2">• Management
• Authority delegation
• Outsourcing/offshoring
• Performance-related remuneration
• Management of change
• Communication channels
Information technology risks
• Importance
• Accuracy
• Computer network access
• Information availability
• Information infrastructure
Integrity risks
• Management fraud
• Employee/third person fraud
• Illegal acts
• Unauthorized use
• Reputation</td><td colspan="2">**Price** - Interest rates
- Currency
- Capital
- Goods
- Financial instruments
- Calculation
Liquidity - Cash flow
- Opportunity costs
- Risk exposure
Other side (business partners)
- Inability to meet obligations
- Exposure
- Settlement
- Quality of products and services
- Quality of property and liability insurance</td></tr>
<tr><td colspan="2">Risks related to information for operational decision-making</td><td colspan="2">Risks related to information for business and financial decision-making</td><td colspan="2">Risks related to information for strategic decision-making</td></tr>
<tr><td colspan="2">• Pricing
• Contractual commitments
• Compliance with the arrangements
• Coordination
• Consistency
• Traceability
• Transparency</td><td colspan="2">• National budget preparation
• Accounting information
• Financial reporting
• Taxes
• Pension insurance
• Investment programs
• Statutory reporting</td><td colspan="2">• Business environment
• Business policy
• Product portfolio
• Value assessment
• Organization structure
• Development strategy
• Allocation of resources
• Planning
• Product life-cycle</td></tr>
</table>

In this project, it is advisable to use the universal risk management model shown in Table 2. Various risk management methods used in specific business areas or processes should also be useful.

Those methods include:

- Control Objectives for Information and related Technology (COBIT) for environments with complex information technology, in which the process survey tool (PST) and risk assessment form (RAF) are also used;
- Federal Deposit Insurance Incorporation Improvement Act (FDICIA) for risk management in banks and other financial organizations;
- CoCo methodology and the Committee of Sponsoring Organization (COSO) assessment methodology which is suitable for all companies and ensures that all risks are identified and appropriately managed. This methodology generally provides the basis for all other methodologies.
- In the area of occupational health and safety, the Preliminary Hazard Analysis (PHA) methods are used. They can also be used in the framework of OHSAS 18001 standards;
- MOSAR systematic risk analysis (Method Organised Systematic Analysis of Risk), and the widely known "Fault Tree Analysis", as well as the Ishikawa or "fish-bone" analysis.
- In environmental protection, the Probabilistic Risk Analysis is often employed, whereby the risk is calculated as event probability multiplied by its consequences.

To conclude, a comprehensive risk management can be handled only by managers and experts, who are well-educated, experienced, prudent, flexible and who follow good practice. The owners and management of corporations, affiliated groups and business systems should be aware that business result depends on successful risk management, and therefore invest more in respective human resources and computer technology which enables the identification, analysis and reduction of risk up to the point when a decision has to be made that high risks (those which are difficult to manage) should be insured with an insurance company.

CONCLUSIONS

Outsourcing is not a question, but a fact. Organizations that want to keep up with the competition in these turbulent times, and timely identify the needs of the market, need to outsource some of their activities. However, they should not forget about the risks of outsourcing.

The entities that are part of critical infrastructure are not an exception. As a rule, these too operate in a free market and have to adhere to its principles. Persons in those entities who are responsible for risks as well as well as integrated security system have to establish appropriate models for the selection and introduction of outsourcing, for the proper functioning of the outsourcing relationship and for the control of this relationship, since in this way, critical infrastructure entities (and certainly all other organizations) optimize the positive effects of outsourcing, and minimize and manage risks of outsourcing to the organization. In the first phase, they should determine, based on expert advice, which activities can be outsourced from the security point of view, and which of them have to be retained within the system of those entities and performed in-house, despite possible benefits of outsourcing. Finally, it should be stressed again that when introducing outsourcing, it is vital to integrate it into business processes, into the system of quality management in accordance with ISO 9001:2008 and security standards, in line with legislation and taking into account those business tools, e.g. benchmarking, business intelligence, 20 key concept, balanced scorecard, human resource management, customer relationship management and social accountability standard (SA 8000), which contribute to positive business results, competitive advantages and the reputation of the contracting authority.

REFERENCES

o Berk, A./Peterlin,J/Ribarič, P. (2005). *Obvladovanje tveganj – skrivnosti celovitega pristopa*. Ljubljana. GV Založba, Založniško podjetje, d.o.o., Zbirka Manager.

o Biringer, B.E., Matalucci, R. V., O Connor, S. L. (2007): *Security Risk Assessment and Management: A Professional Practice Guide for Protecting Buildings and Infrastructures*. New Jersey. John Wiley &Sons.

o Bongard, S. (1994). *Outsourcing - Entscheidungen in der Informationsverarbeitung. Entwicklung eines computergestützten Portfolio-Instrumentariums*. Wiesbaden: Deutscher Universität Verlag.

o Brown, D. (2005). *The Black Book of outsourcing: How to Manage the Changes, Challenges, and Opportunities*.

o Borodzicz, E. (2005). *Risk, Crisis and Security Management*. New York. John Wiley&Sons.

o Broder, J.F. (2006). *Risk Analysis and the Security Survey*. Boston, Oxford. Butterworth-Heinemann o Čaleta, D. (2014). Open dilemmas in counter-terrorism and intelligence exchange cooperation : the regional perspective. V: ČALETA, Denis (ur.), SHEMELLA, Paul (ur.). *Intelligence and combating terrorism : new paradigm and future challenges*. Ljubljana: Institute for Corporative Security Studies; Monterey: Center for Civil-Military Relations, Naval Postgraduate School. 2014, str. 15-24. [COBISS.SI-ID 5102798] .

o Greaver, M. F. (1999). *Strategic Outsourcing: A Structured Approach to Outsourcing Desicions and Initiatives*. New York. AMACOM.

o Hearnden, K., Moore, A. (1999). *The handbook of Business Security*. London, Kogan Page.

o Kehal, H. S., Singh, V. P. (2006). *Outsourcing and Offshoring in the 21st Century: A Socio-Economic Perspective.* London. Idea GroupPublishing.

o Kavčič, K. (2007). *Zunanje izvajanje dejavnosti: analiza slovenskih podjetij.* Koper. Univerza na primorskem. Management št. 4.

o Lewis, T.G. (2006). *Critical Infrastructure Protection in Homeland Security: Defending a Networked Nation.* Wiley InterScience.

o Murray, A. (2007). *Critical Infrastructure: Reliability and Vulnerability (Advances in Spatial Science).*New York. Springer.

o Oshri, I., Kotlarsky, J., Willcocks, L.P. (2009). *The Handbook of Global Outsourcing and Offshoring*. New York, London. Palgrave Macmillan.

o Power, M. J., Desouza, K. C., Bonifazi, C. (2006). *The Outsourcing Handbook: How to Implement Successful Outsourcing Process.* Philadelphia, London. Kogan Page Limited.

o Prezelj, I. (2008). Kopač, E., Svete, U., Grošelj, K., Sotlar, A., Kustec Lipicer, S., Žiberna, A**.,** Kolak, A. *(2008). Definicija in zaščita kritične infrastrukture Republike Slovenije: raziskovalni projekt: končno raziskovalno poročilo*. Ljubljana: Fakulteta za družbene vede, Obramboslovni raziskovalni center, okt. 2008. 526 str.

o Stanger, A. (2011). *One Nation Under Contract: The Outsourcing of American Power and the Future of Foreign Policy*. New Haven, London. Yale University Press.

o Stees, J. (1998). *Outsourcing Security: A Guide for Contracting Services*. Boston, Oxford. Butterwoth-Heinemann.

o Uršič, B. (2006). *Razvoj outsourcinga v podjetju Emo Orodjarna, d.o.o.,* diplomsko delo. Celje. Ekonomsko poslovna fakulteta Univerze v Mariboru.

o Vitasek, K., Ledvard, M., Manrodt, K. B. (2010). Vested Outsourcing: Five Rules That Will Transform Outsourcing. New York, London. Palgrave Macmillan.

o Vršec, M. (2008). *Zaščita kritične infrastrukture v slovenskih organizacijah po evropskih merilih.* Mednarodna konferenca Znanost za trajnostni razvoj, Portorož, 19. 3. do 21. 3 2008, Fakulteta za organizacijske vede, str. 13.

o Vršec, M. (2008). *Redefiniranje ranljivosti in ogroženosti podjetij z izvirnim metodološkim pristopom* [*Redefining the vulnerability and threat to companies with an authentic methodological approach*]. V: Rajkovič, Vladislav in drugi (ur.). 27. mednarodna znanstvena konferenca o razvoju organizacijskih znanosti, Slovenija, Portorož, 19.–21. 3. 2008. *Znanje za trajnostni razvoj: zbornik 27. mednarodne znanstvene konference o razvoju organizacijskih znanosti, Slovenija, Portorož, 19.–21. 3 2008: Proceedings of the 27th International Conference on Organizational Science Development, Slovenia, Portorož, March, 19th-21th, 2008*. Kranj: Moderna organizacija, 2008, str. 3061–3074.

o Vršec, M., Vršec Mir. (2009). *Obvladovanje hudih motenj poslovanja z načrtom neprekinjenega poslovanja in s kriznim načrtom*. Mednarodna konferenca Nove tehnologije, novi izzivi, Portorož, 25.–27. 3. 2009. Fakulteta za organizacijske vede, CD 1575–1587.

o Vršec, M., Vršec, Mir. *(2009) Sistemi in trgi poslovne varnosti.* Študijsko gradivo. Ljubljana. Fakulteta za varnostne vede, p. 311.

o Vršec, M. (2011). *Pomen neprekinjenega poslovanja za poslovno učinkovitost organizacije s poudarkom na kritični infrastrukturi.* International Conference on Days of Corporate Security, Ljubljana. March 23-24th 2011. Ljubljana: Institute for Corporate Security Studies, 9–40.

o VRŠEC, Miran. *The role and risks of outsourcing in the processes of providing corporate security in critical infrastructure.* V: ČALETA, Denis (ur.), SHEMELLA, Paul (ur.). *Counter terrorism challenges regarding the process of critical infrastructure protection*. Ljubljana: Institute for Corporative Security Studies - ICS; Monterey: Center for Civil-Military Relations. 2011, pp. 47-66.

INDEX

A

Application security, 70, 157, 202

B

business continuity analysis phase, 52
business continuity plan, 50–52, 54–56
business entity, 13, 25, 27–28, 30, 90, 92, 98–99, 101–103, 111, 178

C

Communication society, 10, 193–198, 200–201, 205, 208, 212
corporate security, 1–2, 8–14, 47, 71–72, 74, 83–86, 89, 106, 109–111, 129, 131, 135–136, 141–147, 151, 153, 160–162, 165–167, 175, 177–186, 188–189, 217–221, 223, 230–233, 235–236, 239–240, 246–247, 249, 252, 260–262, 284, 291, 298, 321–323, 335, 341
corporate security environment, 10, 219
corporation, 32, 47, 71–72, 84–86, 90, 104, 110–115, 117, 123–124, 126–127, 129, 163, 165–166, 168–169, 211, 218–221, 229, 234, 259–260, 264, 302–303, 305, 310–311, 314, 316–318, 335
Corporatism, 9, 109, 111–113, 115–116, 118–130
corporative security, 2–4, 6–7, 9–10, 12, 35–36, 44–45, 89–93, 95, 103–106, 131, 145, 160, 179, 301–303, 321, 340–341
Crisis, 7, 13–14, 35–45, 50–51, 53–55, 74, 83, 105–106, 110, 139–140, 142–144, 176–177, 183, 185, 221, 235, 238, 240, 299, 321, 332, 334–336, 339
critical infrastructure, 12, 89, 95–96, 101, 107, 186–187, 202–203, 263, 277, 321–323, 325–331, 338–341
Cyber terrorist, 265

cyberattacks, 208–209, 259–260, 263
cyber-crime, 225, 263–264, 270, 273, 276
cybercrime activity, 265
Cybercrime climbs, 260
cyberpower, 201, 205
Cybersecurity, 10, 151, 161, 171, 193, 200–203, 205, 208, 210, 212, 261–263, 266–272, 274–275, 277–278
cyber-specialists, 201
cyber-warfare services, 200
cyberwars, 200

D

danger, 13, 26, 32, 84–85, 94, 166, 171, 175, 177, 195, 201, 237, 248, 335
Data security, 170, 203, 261, 277
detective activity, 8, 73, 78–83, 144–145, 184
Disaster, 7, 35–45, 50–51, 53–54, 218, 231, 299
dissemination of information, 194, 200, 207

E

economic health, 259
Effective management, 47, 272
Emerging Technology, 7, 35, 44–45

F

freedom, 20, 31, 116–117, 129, 166, 193, 196, 212

H

Hacktivism, 265–266
Higher Education, 3, 9, 131–133, 135–136, 141, 145–147

I

institutional basis, 201
integral security, 83, 90, 136
integrated security system, 327, 332, 334, 339

L

legal regulations, 8–9, 55, 89, 91, 100, 162, 183

M

market competition, 18, 30

N

national security, 3, 5–6, 10, 19, 71, 85–86, 89, 92, 94, 107, 131–132, 136, 141, 146, 157, 175–186, 188–189, 193, 200–203, 205, 208–209, 211, 217, 220–221, 236, 240–241, 243, 245–246, 251, 256, 270, 276, 279

Neocorporatism, 124–125

Network security, 63–64, 157, 168, 202, 260, 271

normative frameworks, 91, 95, 101

O

organized crime, 10, 85–86, 142, 144, 160, 172, 180, 204, 217–220, 222–228, 230, 234–236, 247, 249–252, 254, 264–266

outsourcing, 12, 167, 321–331, 334–341

P

Perimeter security, 202

phishing, 302, 307–309, 319

PKI, 301–302, 311–314, 316–318, 320

private security, 8, 15, 71–79, 81–84, 86–87, 89–93, 105–107, 110, 176–177, 180–182, 184, 187–188, 190, 210, 220, 222, 229, 239, 246, 250, 252–253, 256, 262, 332

protecting ICT systems, 259

R

rational decision-making, 280, 291, 294–295

recover data, 195

S

security, 1–15, 18–19, 21–23, 26, 30, 32–33, 35–38, 44–45, 47–50, 57–66, 69–87, 89–95, 99, 103–107, 109–111, 123, 129, 131–137, 139–147, 151–190, 193–194, 196, 198, 200–206, 208–212, 215, 217–224, 227–256, 259–280, 284, 291, 298, 301–303, 305–306, 310, 314, 316–323, 325–327, 329–332, 334–336, 339–341

Security at the endpoints, 202

Security of information and communication systems, 8, 47, 49–50, 60, 65

security risks, 13, 179–181, 183, 185–186, 220, 234, 246, 260, 267–268, 322, 326–327, 329

security threats, 13, 83, 85, 131, 152, 158, 165, 220, 238–239, 241, 246–247, 249–251, 256
social engineering, 12, 185, 227, 265, 301–310, 318–320
Social Media, 7, 35–45, 159, 207, 262, 266
society based on digital technologies, 194
strategic analysis, 288

T

threat assessment, 230, 235
threats, 10–11, 13–14, 35, 44–45, 53, 58–59, 66, 70, 72, 82–85, 90–91, 102, 110, 131, 142, 151–155, 157–158, 160–161, 163, 165–166, 176–177, 180–181, 183, 185–186, 193, 195, 200–202, 205, 208, 212, 217, 219–220, 222–223, 233–235, 237–244, 246–251, 253, 255–256, 259, 261–268, 271–276, 316, 326, 331–332

V

vulnerabilities, 35–36, 40, 44–45, 155, 202, 219, 259–260, 265, 268, 271, 302

W

web-based services, 194