SECURITY IN CENTRAL AND EASTERN EUROPE: CYBERSPACE, POLICE, PRISONS, TRANSPORT, ADDICTIONS, THE MEDIA

Proceedings from the Conference
XLIV CICA: "Security in Europe" – 12th Security Forum Krakow
5–7 June 2018, Kraków, Poland

Edited by:

Prof. Ing. Josef Blažek, Ph.D.
Assoc Prof. Juliusz Piwowarski, Ph.D.
Prof. J. Martín Ramírez, M.D., Ph.D., J.D.

Kraków 2020

Security in Central and Eastern Europe:
cyberspace, police, prisons, transport, addictions, the media

ACKNOWLEDGEMENTS

We would like to express our deep gratitude to Professor J. Martín Ramírez, M.D., Ph.D., J.D., President of CICA International and Chair of the Spanish Pugwash Movement (Peace Nobel Prize 1995), for his efforts to encourage CICA members to the scientific pursuit of security on all levels, from individual to international.

Research and Publishing Institute for Security and Defence Studies
at the University of Public and Individual Security "Apeiron" in Krakow

Security in Central and Eastern Europe: cyberspace, police, prisons, transport, addictions, the media

Proceedings from the Conference
XLIV CICA: "Security in Europe" – 12th Security Forum Krakow
5–7 June 2018, Kraków, Poland

Edited by:
Prof. Ing. Josef Blažek, Ph.D.
Assoc Prof. Juliusz Piwowarski, Ph.D.
Prof. J. Martín Ramírez, M.D., Ph.D., J.D.

Kraków 2020

Security in Central and Eastern Europe: cyberspace, police, prisons, transport, addictions, the media. Proceedings from the Conference XLIV CICA: "Security in Europe" – 12th Security Forum Krakow, 5–7 June 2018, Kraków, Poland

Edited by
Prof. Ing. Josef Blažek, Ph.D.
Assoc Prof. Juliusz Piwowarski, Ph.D.
Prof. J. Martín Ramírez, M.D., Ph.D., J.D.

Conference
XLIV CICA: "Security in Europe" – 12th Security Forum Krakow
5–7 June 2018, Kraków, Poland; hosted by:
University of Public and Individual Security "Apeiron" in Krakow
ul. Krupnicza 3, 31-123 Kraków, Poland
and
Coloquio Internacional sobre Cerebro y Agresion (CICA; International Conferences on Conflict and Aggression)

Language editor and proofreading
Agnieszka Górska

Typesetting and cover
Ewelina Brodziak

Publisher
Research and Publishing Institute for Security and Defence Studies
University of Public and Individual Security "Apeiron" in Krakow
ul. Krupnicza 3
31-123 Kraków
Poland
www.apeiron-wydawnictwo.pl

Funding body
University of Public and Individual Security "Apeiron" in Krakow

Printed edition
110 copies

Digital edition available at
http://apeiron-wydawnictwo.pl/en/e-books/security-in-central-and-eastern-europe-cyber-space-police-prisons-transport-addictions-the-media/

ISBN 978-83-64035-72-2
Kraków 2020

Security in Central and Eastern Europe:
cyberspace, police, prisons, transport, addictions, the media
Proceedings from the Conference
XLIV CICA: "Security in Europe" – 12th Security Forum Krakow
5–7 June 2018, Kraków, Poland

Table of Contents

Publication Standards

Reviewing procedure

Articles submitted to volumes edited and published by Research and Publishing Institute for Security and Defence Studies at the University of Public and Individual Security "Apeiron" in Krakow undergo the following reviewing process:

– **Step 1: Editorial assessment.** The Institute's Editorial Team verify whether the manuscript meets formal requirements and makes the initial assessment of the relevance of the topic to the scope of the research on security.

– **Step 2: Double-blind peer review.** After the article is accepted in Step 1, the Editorial Team delete author's data from the manuscript for the sake of anonymity and forward it to two reviewers (members of the Institute's Editorial Board or other experts in the fields in which the article belongs) for peer review, carried out by filling in a reviewing form. The reviewers must not be affiliated in the author's institution. Double-blind review standard is applied: the author and the reviewers do not know each other's identity and the list of particular articles' reviewers is never published.

– **Step 3: Acceptance, rejection or counselling.** After reviewers submit their recommendations on the forms, an assessment is made whether to accept the article: two positive reviews mean acceptance and two negative ones – rejection. When one positive and one negative review is submitted, the manuscript is sent to the third reviewer. In particularly
difficult cases, e.g. when two very contradictory reviews are submitted, a competent member of the Institute's Editorial Board is consulted for expert advice.

– **Step 4: Final editorial works.** Accepted manuscripts are then worked on by the Editorial Team, in cooperation with the Authors, so that their final form is of sufficient quality. In case the terminology or form of the work is so specialist that certain editorial works go beyond the competences of Technical Editors, a proper Institute's Editorial Board member is contacted, competent in the field in which the article belongs.

Prevention of plagiarism

Research and Publishing Institute for Security and Defence Studies at the University of Public and Individual Security "Apeiron" in Krakow strictly opposes plagiarism. By submitting papers to Institute's publications, authors ensure that they have written entirely original works, and if the work and/or words of others have been used, the authors' duty is to cite or quote them in an appropriate way.

Anti-plagiarism software. To guarantee the originality of the published articles, each paper is checked for plagiarism by an editorial team member using **Plagiat.pl** system – antiplagiarism software used by more than 300 universities in 11 countries on three continents.

Situation 1: Plagiarism detected before publishing. The publisher, in close collaboration with the editors takes all appropriate measures to clarify the situation and to amend the article in question, starting from collecting necessary data and the assessment of the scale of plagiarism, through communication with the author, and ending up with undertaking actions on the manuscript in question (depending on the scale of the problem, these may include corrections, the rejection of the article, or, in most severe cases – even informing relevant authorities). If possible, the editor shall be guided by the proper COPE procedure for detecting plagiarism before publication.

Situation 2: Plagiarism in a published article. If such concerns prove well-founded, the Editorial Team will do their best to cope with the negative results of plagiarism, e.g. by a quick publication of a correction statement or erratum, or, in blatant cases of plagiarism, even by the retraction of the affected work and/or informing relevant authorities. If possible, the editor shall be guided by the proper COPE procedure for detecting plagiarism after publication.

Code of ethics

Research and Publishing Institute for Security and Defence Studies at the University of Public and Individual Security "Apeiron" in Krakow is dedicated to following best practices on ethical matters, errors and retractions. Prevention of publication malpractice is one of the important responsibilities of the Editorial Team. Any kind of unethical behaviour is not acceptable, and, as stated above, the Institute does not tolerate plagiarism in any form. Authors submitting articles to the Institute's publications affirm that man-

uscript contents are original. Furthermore, they warrant that their article has neither been published elsewhere in any language fully or partly, nor is it under review for publication anywhere. The following lists of the responsibilities of authors', editors', reviewers' and publisher's are based on the COPE Code of Conduct for Journal Editors. All the aforementioned participants of the editorial process must also adhere to the ethics-related rules and guidelines given by the Institute's editorial team.

For all parties involved in the act of publishing (authors, editors, reviewers, and the publisher) it is necessary to agree upon the standards of the expected ethical behaviour.

1. Author's responsibilities

Reporting standards. Authors reporting results of original research should present an accurate account of the work performed, as well as an objective discussion of its significance. Underlying data should be represented accurately in the manuscript. A paper should contain sufficient details and references to permit others to replicate the work. Fraudulent or knowingly inaccurate statements are considered unethical behaviour and are unacceptable.

Originality and plagiarism. The authors should ensure that they have written entirely original works, and if the authors have used the work and/or words of others, they ensure that this has been appropriately cited or quoted. The consequences drawn in case plagiarism is detected have been presented before.

Multiple, redundant, or concurrent publication. An author should not in general publish manuscripts describing essentially the same research in more than one volume or journal for primary publication. Parallel submission of the same manuscript to more than one volume or journal is considered unethical publishing behaviour and is unacceptable.

Acknowledgement of sources. Proper acknowledgment of the work of others must always be given. Authors should also cite publications that have been influential in determining the nature of the reported work.

Authorship of a manuscript. Authorship should be limited to those who have made a significant contribution to the conception, design, execution, or interpretation of the reported study. All those who have made significant contributions should be listed as co-authors. Where there are others who have participated in certain substantive aspects of the research project,

they should be named in Acknowledgements section. The 'contact' author should ensure that all appropriate co-authors (according to the above definition) and no inappropriate co-authors are included in the author list of the manuscript, and that all co-authors have seen and approved the final version of the paper and have agreed to its submission for publication. All co-authors must be clearly indicated at the time of manuscript submission. Requests to add co-authors after a manuscript is accepted will require an approval of the editor. Guest authorship and ghostwriting are unacceptable as a manifestation of scientific misconduct. Detected cases, if necessary, will be reported to relevant institutions.

Disclosure and conflicts of interest. All authors should disclose in their manuscript any financial or other substantive conflict of interest that might be construed to influence the results or their interpretation in the manuscript. All sources of financial support for the project should be disclosed.

Fundamental errors in published works. When an author discovers a significant error or inaccuracy in his/her own published work, it is their obligation to promptly notify the work's editor or publisher and cooperate with them to either retract the paper or to publish an appropriate correction statement or erratum.

2. Editor's responsibilities

Publication decisions & accountability. The editor of a work is responsible for deciding which articles submitted to it should be published, and, moreover, is accountable for all the contents of the work. In making these decisions, the editor may be guided by the policies of the Institute's editorial team and/or the policies of the publisher, as well as by the legal requirements regarding libel, copyright infringement, and plagiarism. The editor may confer with other editors or reviewers when making publication decisions. The editor should maintain the integrity of the academic record, preclude business needs from compromising intellectual and ethical standards, and always be willing to publish corrections, clarifications, retractions, and apologies when needed.

Fair play. An editor should evaluate manuscripts for their intellectual content without regard to race, gender, sexual orientation, religious belief, ethnic origin, citizenship, or political philosophy of the author(s).

Confidentiality. An editor and any editorial staff must not disclose any information about a submitted manuscript to anyone other than the author,

reviewers, potential reviewers, other editorial advisors, and the publisher, as appropriate.

Disclosure, conflicts of interest, and other issues. An editor will be guided by COPE's Guidelines for Retracting Articles when considering retracting, issuing expressions of concern about, and issuing corrections pertaining to articles that have been published in volumes edited by the Institute. Unpublished materials disclosed in a submitted manuscript must not be used in an editor's own research without the explicit written consent of the author(s).

3. Reviewer's responsibilities

Contribution to editorial decisions. Peer review assists the editor in making editorial decisions and, through the editorial communication with the author, may also assist the author in improving the manuscript.

Promptness. Any invited referee who feels unqualified to review the research reported in a manuscript or knows that its timely review will be impossible should immediately notify the editor so that alternative reviewers can be contacted.

Confidentiality. Any manuscripts received for review must be treated as confidential documents. They must not be shown to or discussed with others except if authorized by the editor.

Standards of objectivity. Reviews should be conducted objectively. Personal criticism of the author(s) is unacceptable. Reviewers should express their views clearly with appropriate supporting arguments and give a clear conclusion for acceptance or denial of the article. Reviewers must adhere to the procedure of double-blind review procedure adopted by the Publisher, as specified before.

Acknowledgement of sources. Reviewers should identify relevant published work that has not been cited by the author(s). Any statement that an observation, derivation, or argument had been previously reported should be accompanied by the relevant citation. Reviewers should also call to the editor's attention any substantial similarity or overlap between the manuscript under consideration and any other published data of which they have personal knowledge.

Disclosure and conflict of interest. Privileged information or ideas obtained through peer review must be kept confidential and not used for personal advantage. Reviewers should not consider evaluating manuscripts in which they have conflicts of interest resulting from competitive, collaborative, or

other relationships or connections with any of the authors, companies, or institutions connected to the submission.

4. Publisher's responsibilities

Editorial autonomy. Research and Publishing Institute for Security and Defence Studies at the University of Public and Individual Security "Apeiron" in Krakow is committed to working with editors to define clearly the respective roles of publisher and of editors in order to ensure the autonomy of editorial decisions, without influence from advertisers or other commercial partners.

Intellectual property and copyright. Research and Publishing Institute of Security and Defence Studies at the University of Public and Individual Security "Apeiron" in Kraków, Poland ensures the integrity and transparency of each published article with respect to: conflicts of interest, publication and research funding, publication and research ethics, cases of publication and research misconduct, confidentiality, authorship, article corrections, clarifications and retractions, and timely publication of content.

Scientific misconduct. In cases of alleged or proven scientific misconduct, fraudulent publication, or plagiarism, the publisher, in close collaboration with the editors, will take all appropriate measures to clarify the situation and to amend the article in question. This includes the prompt publication of a correction statement or erratum or, in the most severe cases, the retraction of the affected work.

Introduction

The volume ***Security in Central and Eastern Europe: cyberspace, police, prisons, transport, addictions, the media*** is a selection of papers presented on the occasion of the Conference XLIV CICA: "Security in Europe" – 12th Security Forum Krakow (5–7 June 2018, Kraków, Poland). The Conference was held together by University of Public and Individual Security "Apeiron" in Krakow, and Coloquio Internacional sobre Cerebro y Agresion (CICA; International Conferences on Conflict and Aggression), with a simultaneous strong support on the part of Nebrija University in Madrid, Spain.

As the major focus of the Conference was the security of Central and Eastern Europe (CEE), the linking idea of the volume is to present works dealing with the most current **security-related problems encountered by CEE countries**, represented here by **Czech Republic**, **Poland**, **Slovakia**, and **Ukraine**. The first three states, being members of the Visegrad Group, are particularly strongly linked with one another as regards common problems and challenges related to security. Ukraine, in turn, is an important neighbour of the Visegrad Group, shares the majority of security issues with them and at the same time provides its own unique viewpoint on security in the CEE.

In the volume's papers, **research on security is carried out within the framework of *security sciences***, which, in Poland and increasingly in other countries in CEE and beyond, is an **emerging scientific discipline**, or at least a new research trend that enjoys a status of an independent discipline. Along with *security sciences*, there is also **an older, internationally known area of science called *security studies***, which is considered worldwide a subfield of the discipline of political science. *Security studies* are, without

doubt, very meritorious to research on security; however, *security sciences* are unique owing to their methodology which allows for the scientific investigation of *security subjects* within the full spectrum of tools offered by social sciences. It should be noted that in *security studies*, a similar opportunity became available as late as in the times of the Copenhagen School, that extended the notion of a *security subject* onto not only states, but also social groups and individuals.

The contributors were not arbitrarily assigned the topics of their papers; they chose them on their own, basing on their own expert assessment of what the most burning security-related issues are in their countries and their immediate neighbourhood. Thus, six main areas were addressed – ***cyberspace***; uniformed services including servicepeople of ***police*** and ***prisons***; ***transport***; ***addictions***; and ***the media***.

The topic of ***cyberspace*** is addressed by two papers. The introductory essay, ***Prolegomena for Studying Security Culture in Cybersociety*** by Juliusz Piwowarski and Radosława Rodasik, investigates the problematics of security culture in the modern cybersociety (in the ***international*** as well as ***national*** perspective), and at the same time contains a valuable guide to the notions and sources related to the aforementioned **Polish** and increasingly international concept of *security sciences*.

The paper ***Cyber Attacks on Critical Information Infrastructure: Definitions, Threats and the Czech Perspective*** by Josef Požár enriches the general perspective on ***cyberspace***, sketched by Piwowarski and Rodasik, with terms of a more technical nature and with the ***national*** viewpoint of another CEE country: the **Czech Republic**. Požár depicts in a comprehensive way the up-to-date cybersecurity system in the Czech Republic, provides locally relevant definitions of cybersecurity terms as included in Czech expert publications on cybersecurity, and pays much attention to the role of the ***uniformed services***, especially the ***police***.

The topic of the ***police***, in this volume investigated specifically from the ***national*** perspective of the **Czech Republic**, is more comprehensively addressed in the paper ***Fuzzy Problems in Security Management: New Threats and the Importance of Tacit Knowledge in the Police of the Czech Republic*** by Dana Junková and Milan Kný. The authors begin with another valuable passage on the methodology of *security sciences*, and then proceed to the discussion on the role of tacit knowledge in the education, training and practical work of Czech policepeople.

Another current topic discussed within the area of ***uniformed services*** is ***prisons***; this is represented by another contribution dealing with the ***national*** security of the **Czech Republic**. ***Radicalisation – Def inition, Models, Detection in Czech Prisons*** by Štěpán Strnad and Štefan Danics offers an insight into how radicalised prisoners are identified in the Czech prison system. Much place is devoted to an innovative project of the Czech police named SAIRO (Systém analytické identifikace radikalizovaných osob – System of Analytical Identification of Radicalised Individuals).

The area of ***transport*** security is discussed from the ***national*** **Ukrainian** perspective; as a prominent country in CEE region and an important neighbour of the Visegrad Group, Ukraine is a vital contributor to the discussion on CEE security. In the paper titled ***Safe Transportation of Goods in the Supply Chain of Contemporary Ukraine: Risk Management and Means of Loading Safety***, Larysa Yankovska and Ilona Petryk provide the reader with a vast bulk of information on the reality of cargo transport in Ukraine and related security issues, including the legal, technological, and managerial aspects. After identifying the local challenges to load security, the authors apply the methodology of risk management to adress the identified problems.

As regards ***individual*** security issues related to ***addictions***, in her contribution ***Why doesn't prevention work? Drug and alcohol prevention among adolescents in Europe***, Marzanna Farnicka presents a comprehensive picture of prevention programmes applied in Europe to combat problems related to the use of alcohol and other drugs among youth. A certain emphasis is put here on the local situation in **Poland**, reflected in the empirical data collected in a survey carried out by Polish Agency for Solving Alcohol Problems (PARPA).

The final article, dedicated to linking security and ***the media***, brings the readers back to the wide ***international*** perspective. The work ***The Role of the Media in Multitrack Diplomacy*** by Rastislav Kazansky discusses the meanders of conflict resolution – a topic so important to international security – referring to two important notions applied in international relations: multitrack diplomacy and the CNN effect. Much as the contribution by a **Slovak** researcher addresses the topic from the global perspective, not focusing on a narrower national viewpoint of his country, the paper is in fact based on a number of representative sources from Slovak subject literature, and thus constitutes an insight into the local CEE point of view on the discussed notions.

On behalf of all the authors, I do hope that the current volume will equip members of the **international community of researchers in security** – especially those from beyond CEE – with knowledge on up-to-date CEE security-related problems, attitudes and methodological tools. This knowledge is important not only for the better insight into the research topics related to the region and their possible links with respective global topics; this knowledge is also **a small but irreplaceable piece of information necessary in the common global struggle for maintaining security** of individuals, communities and nations throughout the world.

Assoc. Prof. Juliusz Piwowarski, Ph.D.

Head of Research and Publishing Institute for Security and Defence Studies
at the University of Public and Individual Security "Apeiron" in Krakow

SECURITY SCIENCES AND SECURITY CULTURE IN CEE AND THE WORLD

**SECURITY IN CENTRAL AND EASTERN EUROPE:
CYBERSPACE, POLICE, PRISONS, TRANSPORT, ADDICTIONS, THE MEDIA**
Proceedings from the Conference
XLIV CICA: "Security in Europe" – 12th Security Forum Krakow
5–7 June 2018, Kraków, Poland
2020 (20–49); https://doi.org/10.24356/proceedings2018/1

Prolegomena for Studying Security Culture in Cybersociety

Juliusz Piwowarski*
Radosława Rodasik**

ABSTRACT

The authors of the paper point to the changes that humankind is witnessing in the contemporary cybersociety and discuss the possible impact of these changes on human social security. The paper begins from sketching the theoretical framework for discussing security: first, main ideas of the Copenhagen school of security studies is introduced, and then ideas of the Polish researchers in *security sciences* follow, including the core concepts of Polish *security sciences*, such as *security culture* with its "three streams of energy", or *security environment*. Then the authors introduce the changes brought about to the humankind with the advent of the digital era, including

* Assoc. Prof. Juliusz Piwowarski, Ph.D., University of Public and Individual Security "Apeiron" in Krakow, Kraków, Poland; correspondence address: ul. Krupnicza 3, 31-123 Krakow, Poland; email: juliuszpiwowarski@apeiron.edu.pl
** Radosława Rodasik, M.A., University of Public and Individual Security "Apeiron" in Krakow, Kraków, Poland.

the changes in human communication. Finally, they move on to discuss the risks, dangers, and challenges to proper development that a *security subject* may meet in the modern, cybernetic world – including bad quality of information, Internet addiction or the deterioration of intellectual skills – and discuss them in the light of the theory of *security sciences* and the possibilities of the further development of *security culture*.

ARTICLE INFO

Article history
Received: 30.09.2019 Accepted: 7.01.2020

Keywords
security, security culture, social security, cybersociety, communication

Introduction: *security sectors*, *security culture* and *security environment*

In his article *New Patterns of Global Security in the Twenty-First Century*,[1] Barry Buzan showed a list of concepts he has identified – security spheres, which he called *security sectors*. In the initial proposal of Copenhagen school of security studies (of which Buzan was a prominent representative), which came into being at the turn of the 1980s and 1990s, the following sectors of national security were, in turn, presented:

1) political sector,
2) military sector,
3) economic sector,
4) socio-cultural sector,
5) ecological sector.

The idea of *security sectors* is a very important part of Buzan's concept of security, which, together with the concept of three *security scales*, is an important distinguishing feature of the Copenhagen school. Buzan, consistently following the holistic research formula, claimed that security sectors do not operate in isolation from each other and that *de facto* they are sectors of the specific, established human heritage, i.e. *security culture*.

[1] B. Buzan, *New Patterns of Global Security in the Twenty-First Century*, "International Affairs", 1991, vol. 67, no. 3, pp. 431–451.

Each of *security sectors* describes the area aggregating a given group of *security issues* and the priorities within this group. At the same time, all these spheres are intertwined together in a strong network of connections. It should be noted that the founders of the Copenhagen school, while searching for the golden mean for their research, strongly emphasized the importance of the sphere of human identity, i.e. the *socio-cultural sector*, for the achievements determining the level of *national security culture*, which makes their idea close to the concept of *security culture* elaborated by Polish scholars within the research framework of security sciences.[2]

As Batorowska noted, referring directly to the issues of information security culture, "the shaping of the aforementioned components of *security culture* is closely related to education [and accompanying upbringing] for security in the area of information and knowledge management. In an environment of redundancy of information and its use to manipulate attitudes and behaviour of people it is difficult not to connect *security culture* with the information culture of an individual, an organization, and a nation".[3]

It can be said that virtually all human-made societies, even those that were built a long time ago, are to some extent information societies. They had to be information societies in order that the second energy stream of security culture[4] (representing the social-communal aspect of security) functioned well in them, which was necessary to ensure the successful cooperation of these societies' members in social[5], natural[6] and technical[7] reality. The three streams of energy of security culture give people the chance to survive in these three realities. This is done mainly by stimulating and sustaining those individual and group tendencies which can serve as a driving

[2] More on the Polish concept of *security culture* can be found here: J. Piwowarski, *Three pillars of security culture*, "Kultura Bezpieczeństwa. Nauka – Praktyka – Refleksje", 2018, no. 29(29), pp. 22–32, https://doi.org/10.24356/KB/19/2.

[3] H. Batorowska, *Kultura bezpieczeństwa informacyjnego*, "Edukacja – Technika – Informatyka", 2018, no. 1/23/2018, pp. 92–100, https://doi.org/10.15584/eti.2018.1.11, https://repozytorium.ur.edu.pl/bitstream/handle/item/3957/11%20batorowska-kultura%20bezpieczeństwa.pdf?sequence=1sAllowed=y (accessed 22.10.2019).

[4] More on the concept of the three components of security culture can be found in: J. Piwowarski, *Three pillars…*, *op. cit.*

[5] J.R. Searle, *The Construction of Social Reality*, New York 1996; A. Schütz, *The Phenomenology of the Social World*, Evanston 1997.

[6] G.E. Kaebnick, *Humans in Nature: The World As We Find It and the World As We Create It*, New York 2013.

[7] R. Garud, *The Social Construction of Technological Reality*, London 2018.

force for building human security and for maintaining its multi-faceted development.[8]

Security culture can be defined as a set of fixed works of human that serve human's broadly understood (in both the non-military and military sense) immunity, protection and defence. *Security culture* has a threefold nature: it consists of three "streams of energy": mental-spiritual, organisational-legal, and material. *Security culture* enables individual and group *security subjects* to:[9]

- control dangers,
- regain the desired level of security in case it declines,
- optimise security sectors by harmonising the potentials of these sectors,
- stimulate, both on the social and on the personal scale, the need for development and self-improvement, as well as the motivation for taking individual and group actions to meet these needs by building resilience and defence skills in individual and group security subjects.

The concept of *security culture*, with its three streams of energy: individual, communal and material, bases on the ideas of such figures of science as Alfred Louis Kroeber[10], Marian Cieślarczyk[11], and Stanisław Jarmoszko.[12] The humanistic and personal dimension of this concept has then been researched by Teresa Grabińska,[13] Krzysztof Drabik,[14] or Mariusz Kubiak,[15]

[8] J. Piwowarski, *Nauki o bezpieczeństwie. Kultura bezpieczeństwa i redefinicja środowiska bezpieczeństwa*, Warszawa 2020; *eadem*, *The security (culture) rhombus. Redefining security environment*, "Kultura Bezpieczeństwa", 2019, no. 34, 141–154, https://doi.org/10.5604/01.3001.0013.5190; discussion at the international Security Forum conference XIV & CICA XLIX, Kraków 2019.

[9] M. Cieślarczyk, *Kultura bezpieczeństwa i obronności*, Siedlce 2011; J. Piwowarski, *Three pillars of security culture*, "Kultura Bezpieczeństwa. Nauka – Praktyka – Refleksje", 2018, no. 29(29), pp. 22–32, https://doi.org/10.24356/KB/19/2.

[10] A.L. Kroeber, *The Nature of Culture*, Chicago 1952.

[11] M. Cieślarczyk, *Kultura…*, *op. cit.*

[12] S. Jarmoszko, *Status kultury strategicznej w kontekście badania i kreowania kultury bezpieczeństwa*, [in:] *Elementy teorii i praktyki transdyscyplinarnych problemów bezpieczeństwa*, A. Filipek (ed.), vol. II, Siedlce 2014, pp. 289–308.

[13] T. Grabińska, *Etyka a bezpieczeństwo personalne*, Wrocław 2013.

[14] K. Drabik, *Dekonstrukcyjne i konstrukcyjne funkcje zagrożeń w kształtowaniu bezpieczeństwa personalnego*, [in:] *Problemy bezpieczeństwa i zarządzania kryzysowego*, M.R. Gogolin (ed.), vol. II, Bydgoszcz 2019, pp. 44–55.

[15] M. Kubiak, *Filozofia bezpieczeństwa personalnego i strukturalnego: tradycja – współczesność – nowe wyzwania*, Siedlce 2007.

and its systemic and legal dimension has been explored by Waldemar Kitler.[16]

As regards foreign scholars, parallels should be perceived between the concept of *security culture* and the notion of *security climate* in Dove Zohar's research.[17] Nick Pidgeon, in turn, when investigating the relationship between safety and culture in organizations, applies the term *safety culture*; so does Stian Antonsen in his book *Safety Culture: Theory, Method and Improvement*.[18]

When analyzing the problems of *security culture*, it is worthwhile to reflect on the very phenomenon of culture as such. It is because culture is a social phenomenon that determines the development of human treated as a *security subject*. Thus, culture encompasses human's creative activity (which is the essence of *culture* itself) seen in the context of *values* sought by him/her; his/her *needs* and *interests* carried out in connection with these needs; the *challenges* and *opportunities* he/she faces; the *risks* that he/she encounters, the *dangers* threatening him/her, and the *culture of security* that he/she builds.

All of the abovementioned issues are the components of the *security environment* that surrounds a given *security subject*. The *security environment* is a set of "the external and internal, military and non-military (i.e. civilian) conditions of security (i.e. the conditions under which the security-related interests and objectives of a given entity are fulfilled), that are characterised by the four basic categories of opportunities, challenges, risks and threats".[19]

The components of the *security environment* listed in the abovementioned definition are explained in the *White Paper on National Security of the Republic of Poland*: "*Security opportunities* – circumstances (phenomena and processes in the security environment) independent of the will of the

[16] W. Kitler, *Transdyscyplinarność badań w naukach o bezpieczeństwie i w naukach o obronności*, [in:] *Metodologiczne i dydaktyczne aspekty bezpieczeństwa narodowego*, W. Kitler, T. Kośmider (eds), Warszawa 2015, pp. 159–177.

[17] D. Zohar, *Safety climate in industrial organizations: Theoretical and applied implications*, "Journal of Applied Psychology", 1980, no. 65(1), pp. 96–102, https://doi.org/10.1037/0021-9010.65.1.96.

[18] N. Pidgeon, *Safety culture and risk management in organizations*, "Journal of Cross-Cultural Psychology", 1991, no. 22, pp. 129–140, https://doi.org/10.1177/0022022191221009; S. Antonsen, *Safety Culture: Theory, Method and Improvement*, Burlington 2009.

[19] *Biała Księga Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej*, Warszawa 2013, p. 247.

subject which are conducive to the achievement of the subject's security interests and objectives. *Security challenges* – problem situations generating decision-making dilemmas faced by an entity in resolving security issues. When improperly addressed or underestimated, security challenges can ultimately turn into real security threats. *Security risks* – possibilities of negative consequences of one's own actions in the area of security for a given entity. *Security threats* – direct or indirect destructive impacts on an entity. The most classic factor of the security environment; a distinction is made between potential and real threats; subjective and objective; external and internal; military and non-military; crisis-related and war-related; intentional and accidental (random)".[20]

Security in the modern society

For a scholar researching security and threats, one of the security environments is *cybersecurity* – a security environment in which the process of communication is an important component of the power manifested by the aforementioned *second stream of energy* of *security culture*, i.e. the aspect of *security culture* relating to the potentials of human social communities.

What is important, this process of communication is constantly evolving, it is subject to changes with the development of technology, so it is always a timely research topic. In the context of the considerations conducted here, it is worth noting the common etymology of the word *communication* (in Polish: "komunikowanie (się)") and *community* (in Polish: "społeczność, wspólnota").[21] Today human has to deal with innovative ways of communication and non-traditional social forms accompanying new methods of communication. It is highly probable that these phenomena need the creation of new theories concerning the ontology of the present-day social world.[22]

Just as the Industrial Revolution, initiated in the 18th century in England and Scotland and involving technological, economic and socio-cultural changes, had a huge impact on human societies, so does today the digital revolution. The actual beginning and later development of the information

[20] *Ibidem*, p. 248.

[21] C.H. Vogl, *The Art of Community: Seven Principles for Belonging*, Oakland 2016.

[22] J. Piwowarski, *Społeczeństwo informacyjne a kultura bezpieczeństwa*, "Zeszyt Naukowy WSBPI »Apeiron« w Krakowie", 2011, no. 6, pp. 161–174.

society was closely connected with the technological revolution of the second half of the 20th century. Here too, a digression: an observer of the history of socio-cultural change may be surprised by the acceleration of the pace of subsequent changes. Goban-Klas and Sienkiewicz presented the history of humankind until 2000 in the form of a symbolic clock. The clock captures human history within one symbolic day, so one hour corresponds to one and a half thousand years.

According to this model, people at midnight communicated with each other through words, gestures and facial expressions, at 8.00 they mastered the technique of painting pictures, and only at 20.40 – the use of hieroglyphics. Alphabet-based writing was used at 21.38, and the printed message at 23.30. The personal computer started working as late as 49 seconds before midnight.[23] Now, a few seconds after midnight, we are dealing with the digitalization of the world, accessible to the average person.

Perhaps the most serious influence on the emergence of the idea already widely known today as the information society was the American sociologist Daniel Bell.[24] In creating this innovative concept in the 1960s and 1970s, Bell put forward a thesis about the existence of a new social need to take an innovative direction in the process of further socio-cultural change. By claiming this, Bell, in his own opinion, pointed out the direction that his country, the United States, was to take in order to ensure to itself long years of economic growth and to gain a significant advantage on the international stage in the newly created, technogenic world of computers and digitisation. Similarly, the adoption and stimulation of a new social, cultural and economic developmental shift related to digitalization, according to Bell, was to provide giant corporations with an optimal strategy that would allow them to multiply the profitability of the expected results.

Bell pointed out that his thesis indicating de facto the need to build not only a completely new sector of industry, but above all a new sphere of culture – this was another thesis within his theory – was not an extrapolation of the existing trends, but it indicated completely new rules and measures necessary for the social world to change the rules of its organization.[25] He

[23] T. Goban-Klas, P. Sienkiewicz, *Społeczeństwo informacyjne: szanse, zagrożenia, wyzwania*, Kraków 1999.

[24] F. Webster, *Theories of the Information Society*, London–New York 2002, p. 314.

[25] D. Bell, *The Third Technological Revolution and its Possible Socioeconomic Consequences*, "Dissent", 1989, Spring, pp. 164–167.

also stressed that, in his opinion, the socio-cultural changes caused by the information revolution are inevitable.

Castells, in turn, defined the information society as a new form of further human development. He considered that it was being created contemporarily, in the process of transforming the free market economy. He also assumed that the information society is organized around various processes in which people are involved and which are determined by historical relationships concerning such components of the social world as production, experience and power. The *network society*, he claimed, was the society of indignation and hope of the social movements being parts of the network, in which there was a change in the concepts of time and space – real, linear time was replaced by timelessness and space by the flow of information.[26]

According to the futurologist Alvin Toffler, the so-called *future shock* is to come,[27] which means that the rapid development of civilization and technology may cause a psychological shock in stabilized societies. According to Toffler, future shock is experienced by those who – unprepared to accept new cultural symbols – suddenly face the necessity of getting rid of everything they are already accustomed to overnight.[28] In this situation, a large part of the population is unable to get out of its comfort zone and is therefore not ready for change, which provokes conflicts. Toffler also points out that knowledge does not have to wear out physically, as it can be compressed in the form of symbols and abstract representations that can be placed on portable devices, external or digital. He was not wrong in his forecasts – today we have Big Data, flash drives, and digital clouds.

Vannevar Bush was one of the visionaries who had even earlier described and felt the need for an era of "electronic brains". In his essay *As we may think*, published in 1945 in "The Atlantic", Bush presented a vision of a system that would serve as a prosthesis of the human mind, and called it 'memex'. Actually, it was a harbinger of today's Internet.[29] Memex is today reflected in digital clouds, social networking sites, etc. (e.g. Facebook, on which 300 million photos are uploaded every day), and in the fact that we send 204 million e-mails a day and in pockets and bags we carry about

[26] M. Castells, *Społeczeństwo sieci*, Warszawa 2008, p. 31; M. Kowalczyk, *Cyfrowe Państwo. Uwarunkowania i perspektywy*, Warszawa 2019, p. 124.

[27] A. Toffler, *Szok przyszłości*, Warszawa 1970.

[28] *Ibidem*.

[29] V. Bush, *As we may think*, „The Atlantic", 1945, http://www.theatlantic.com/magazine/archive/1945/07/as-we-may-think/303881/ (accessed 22.10.2019).

5 billion smart devices.[30] These are peculiar contemporary implants of our memory of the future. So, how to deal with so many memories, stimuli and the need to remember, or capture the moment? What happens if the drive breaks down and the cloud is destroyed by a hacker? The answer will not be prevention but rather planning and designing an appropriate infrastructure for secure cyberspace.

The digital revolution and its social impact

The digital revolution began in the mid-20th century and continues uninterruptedly. Incidentally, this phenomenon and its development clearly show that the implementation function of social sciences, which is often underestimated, is not just a pipe dream. The digital revolution began with the invention of a device which was an addition to the already existing culture and, at the same time, its completely new element. It became a new element of the physical *third stream of security culture*. This device was the first digital machine. First digital machines were used by the military security sector. They were complicated devices for that time, functioning thanks to the knowledge discovered by mathematicians. They processed information and performed arithmetic and logical operations on numbers and symbols.

Such a machine was ENIAC, or Electronic Numerical Integrator And Computer, which was constructed between 1943 and 1945 by John Presper Eckert (1919–1995) and John William Mauchly (1907–1980), both engineers and researchers who worked at the University of Pennsylvania in the United States. For the sake of scientific objectivity, it should be added that ENIAC, considered by many to be the first electronic computer in the world, was designed and used mainly for calculations carried out in the ballistic laboratory of the US Army. ENIAC's first task was to investigate the possibility of damaging thermonuclear weapons designed at the end of the Second World War. ENIAC was completed and commissioned for the first time in December 1945.

Until 1975, ENIAC was widely recognized as the first electronic computer in the world. Nowadays – which could happen only after some time, after declassifying certain data, among others those from British archives – other inventors are also competing for the title of the pioneer in

[30] J. Korus, *Mglista przyszłość naszych wspomnień*, "Newsweek. Tajemnice przyszłości", 1/2019, pp. 102–107.

the construction of electronic computers. These include the mathematical genius Alan Turing[31] (the creator of the British computer Colossus and the author of the test that determined the ability of a machine to use natural language[32]) as well as the German engineer and inventor who pioneered computer science, Konrad Zuse.[33] During World War II Zuse was a designer of German electronic computers belonging to the so-called Z series, with the most famous Z3 device.

The ABC (Atanasoff-Berry Computer) device, which was built in Iowa State University, is also claimed to be one of the first electronic computers in the world.[34] It was built in the period from 1937 to 1942. Its designer was an American engineer of Bulgarian origin, John Vincent Atanasoff, who worked on the device together with his assistant Clifford Berry.

Regardless of which of the abovementioned computers appeared as first in the third stream of security culture, thus initiating in the social world the process of passing through the great digital revolution, it was with the introduction, at the end of the first half of the 20th century, of these devices to the arms race in the arena of military security sector that the era of dynamic development of computational technology began.

[31] Alan Mathison Turing (1912–1954) – British mathematician and cryptologist, creator of the concept of the Turing machine, one of the creators and pioneers of computer science, also considered the father of the concept of artificial intelligence. In 2014, for the first time in history, the supercomputer deceived people and passed the Turing test. The program "pretended" to be 13-year-old Eugene Goostman and after a few minutes of chat convinced the so-called judges that it is a human being. This test, created by Alan Turing, was first published in 1950. (See: A. Turing, *Computing Machinery and Intelligence*, "Mind", vol. LIX, no. 236, October 1950, pp. 433–460, http://web.archive.org/web/20110726153108/http://orium.homelinux.org/paper/turingai.pdf (accessed 22.10.2019)).

[32] Colossus – a project of a series of digital machines based on the theoretical foundations of Alan Turing's work, managed by Max Newman and Tommy Flowers, with the participation of Turing; the Colossus computer was built for the army in 1943 in the Bletchley Park cryptographic centre and was used to work out German ciphers.

[33] Konrad Zuse (1910–1995) – constructor of the first computer, whose functioning was based on binary system; in 1936 he patented mechanical memory; he also constructed electromechanical and electronic counting machines, used e.g. for designing wings of airplanes.

[34] Atanasoff-Berry Computer, ABC – an electronic machine for solving systems of linear algebraic equations, thanks to the use of electronic tubes, recognized as a prototype of an electronic digital computer; working very slowly, under constant supervision of a human being; nevertheless, it was about a thousand times faster than mechanical devices.

Computational technology has both offered widespread access to the unprecedented amounts of information at very short notice, and provided unprecedented giant facilities for people to communicate with one another, thereby also boosting the power of the *second energy stream of the security culture*.

It is worth mentioning here that in the 1960s, Robert McNamara, the then US Secretary of Defense, who was a mathematician by education, permanently introduced in the Pentagon management methods based on a decisive improvement in the "relationship" between human and computer. This shows new tendencies in mutual permeation of the three *energy streams of the security culture* – both the *first energy stream* and the *second energy stream* blend with the third one.

In the mid-1960s, more than 50% of American GDP was generated by those employed in services such as information production, processing and distribution.[35] In the USA, as a result of the dynamic development of the information society based on the communication revolution, there has been a transition to "a public discussion on the use of the latest technology for the benefit of society. It was initiated by the US government, which in the 1970s began legislative and organizational work to promote the idea of information society".[36]

The National Academy of Sciences of the USA published a report in 1979 on the directions of changes introduced along with the development of the country's digitalization. In turn, the US government introduced changes in the legal and fiscal system, and then limited public intervention in the development of the information society, for which science and business were to be responsible.

In 1993, President Bill Clinton's administration implemented the National Information Infrastructure strategy. The strategy was about building national infrastructure of ICT networks (so called *information highway*) and enabling universal, commercial access of all citizens to ICT. As a result of these activities, already in 2006 out of 100 companies with the largest capital, more than half operated in the telecommunications and IT sectors.[37]

[35] K. Doktorowicz, *Europejski model społeczeństwa informacyjnego. Polityczna strategia Unii Europejskiej w kontekście globalnych problemów wieku informacji*, Katowice 2005, p. 61.

[36] M. Nowina-Konopka, *Istota i rozwój społeczeństwa informacyjnego*, [in:] T. Białobłocki, J. Moroz, M. Nowina-Konopka, L. Zacher, *Społeczeństwo Informacyjne. Istota, rozwój, wyzwania*, Warszawa 2006, p. 20.

[37] See: K. Doktorowicz, *Europejski model społeczeństwa informacyjnego. Polityczna strategia Unii Europejskiej w kontekście globalnych problemów wieku informacji*, Katowice 2005.

Problems for *security culture* in the digital era

In the research on *security culture* in the postmodern information society, two opposing socio-cultural tendencies become apparent. Firstly, both *security culture* and modern technology, especially digital technology, demand a higher and higher level of perfectionism from people in many aspects. Perfectionism and moral integrity are not, unfortunately, among the strengths of the spirit of our times. Despite the fact that modern technology requires more and more perfection, good cooperation and reliability from the user, the current educational systems, the media, entertainment and ubiquitous populism strongly degrade the competences we need. Secondly, postmodern trends direct human behaviour towards a fake version of freedom, which, among other things, is supposed to allow human to free himself/herself from the cultural ties that allegedly constrain his/her nature, from the obligations imposed on him/her, and from the requirements to be precise, punctual, and educated.

A crisis of values and axiological relativism, together with today's speed and numerousness of digital devices, may in a moment bring losses unimaginable in their size, effects and range.

The authors point out reservations about utopian and premature paeans concerning the idea of global, ideal civil society. Let us take into account several sources of threats to security culture caused by avalanche-like, spontaneous and uncontrolled development of information networks, and billions of more and more socially atomized human individuals living in the world.

Threats to *personal security* posed by the digital media

Firstly, billions of human beings living on Earth would have to form a society, or at least a number of harmonious social organisms, based on the social paradigm of consensus. Secondly, an avalanche of information, not properly filtered by incompetent audiences, may take the form of contemporary Pandora's box. Recipients are becoming increasingly incompetent because today the planned process of moral and intellectual development of human, which was conducted in the traditional school and based, among other things, on literature properly matched to age and educational and social needs, was replaced by chaotic choices of information, often pictorial and deprived of deepened intellectual content, derived from the Internet or television. There is a vast amount of such information and data on the Internet; much of this information is devoid of any substantial value,

a large part of it is not interpretable, and there is also a layer of information that constitutes a threat because it is simply false information. The average child for whom parents do not have enough time almost every day, is often recklessly "entrusted", together with all the complicated problems concerning his/her maturation, to entertainment, TV commercials, telephones and computers. It is not a problem for him/her to gain access to e.g. violent virtual games, sophisticated pornography films or bestial torture as part of his/her relaxation or the satiation of his/her curiosity.

People brought up on visual media have an impoverished perception compared to those who can read a traditional book with satisfaction and understanding. These "digital illiterate" people have a suboptimally shortened focus time, which, in education, has negative personal and social consequences.[38] These young people, who are still young today, will soon become parents, leaders, doctors and members of the uniformed services. Their contribution to *security culture*, with their uncontrolled rejection, due to the misuse of the Internet, of a solid, genuinely autonomous education, may soon prove to be very questionable.

Nothing in the human development can replace the highly advanced training of the brain associated with the transformation of abstract, preferably handwritten signs called letters, first into single sounds, then into words and concepts, then into sentences and whole images of events built in one's own free imagination, not yet amputated by the imposition of the ready-made creations of mass entertainment providers.

Human is a haptic being.[39] Today, multimedia screens are thoughtlessly "allowed" by human beings to conduct excessive, almost unlimited exploration and exploitation of their brains, putting these brains to sleep, and choking the imagination hidden in them. These deficiencies are increasingly being accompanied by speech and logic impairments and, what is even worse, by serious deficiencies in the part of human imagination which is supposed to support the ability to feel compassionate and to deepen emotional intelligence (maturity).

[38] Cf. K. Krzysztofek, *Rdzeń kultury a cywilizacje*, "Transformacje", 1995/1996, no. 3/4, p. 151.

[39] M. Grunwald, *Homo hapticus. Dlaczego nie możemy żyć bez zmysłu dotyku*, Kraków 2019.

In the human cerebral cortex, information from the sensory organs of all senses is received and analysed in harmonised data packages, for example:

vision + hearing + smell + touch + perception of space (depth, distance).

In this part of the brain, associative processes based on the wealth of sensory experiences take place, and thus instructions are given to determine the motor reactions. The most common senses used by the Internet user are sight and hearing. Visual and auditory stimuli are received, processed and then synthesized. This is the first stage of information processing. The systems of stimuli reflect fragments of reality that surrounds us and is perceived by us. Experiments have shown that through physical or mental activity the brain builds new neural circuits or strengthens the existing ones, but at the same time those that are not used can weaken or even disappear.

If we stop practicing our mental abilities – among others, the psychophysical ones – then not only do we forget them, but also, on the maps of our brains, the spaces assigned to them are going to be taken over by other skills, "easier" but in fact more primitive – i.e. those that we are using at a given moment.

It is known that the abilities for reasoning, perception and action are determined not only by genes and important childhood experiences, according to the "rule of first associations", but they are subject to change throughout human life.

The technology available to people to help them perceive reality is also constantly changing. Today, human is at the stage where he/she is forced to operate more and more information, and in addition, this information is obtained in very short time. The speed at which a given entity obtains information and the accuracy of this information significantly affects, for example, a company's economic result, one's decisions concerning future plans and actions, the management of one's own time, or even the choice of one's own lifestyle or entertainment preferences.

The Internet and problems with the development of a *security subject*

The Internet is a special system which very efficiently and, if necessary, repeatedly, juxtaposes a quick question and a quick answer with each

other. By clicking on another link, behind which stands the next portion of information, the computer user receives answers to further and further questions asked by him/her or moves on to the next stage of reaching the information he/she needs. It also requires a quick verification of every element that belongs to this fast flow of information.

Very often, however, Internet information is superficial, of low cognitive value, and sometimes the data received is unsatisfactory. If the subject of action does not receive an answer to his/her question, he/she clicks on the next link. This process lasts until information is obtained which is satisfactory for the subject of the action. The viewed content can take many forms: changing texts, images, videos, links marked in colour or highlighted, virtual buttons that encourage one to click on them. Thus, in general, these simple, physical and mental activities are repeated, especially when acting quickly.

Usually, the content of the displayed information is analysed in a superficial way. The Internet provides one with regularly recurring, interactive sensory and cognitive stimuli. Eyesight tracks only those elements displayed on the screen that are attractive to the viewer. Rapidly changing content on the screen is not conducive to concentration, which is needed to analyse it reliably. On the contrary, it is conducive to superficial reading, thought chaos and superficial learning.

In such a situation, the subject of action, who may at the same time be considered as a *security subject*, focuses intensively on blinking images. At the same time, the messages and stimuli delivered to him/her at a staggering rate and thus difficult to deal with in a reflective manner, have a distracting effect on him/her. The characteristic cacophony of stimuli characteristic of the Internet occupies the conscious and unconscious mind of the subject, not allowing him/her to think deeply and thoroughly, nor to think fully creatively.[40]

The more often one visits websites, the less often one becomes familiar with carefully thought-out and structured datasets, devised by responsible, non-anonymous authors. Such datasets are offered to us by books.

Web browsing is a much simpler process than reading a traditional book; in the latter case one usually has to go to a bookstore to obtain one, and then one leafs through the book, reads it, and sometimes also takes notes – not using the mechanical copy-paste function, but tensioning one's hand in the activity of writing. What is needed here is a greater concentration

[40] N. Carr, *Płytki umysł. Jak Internet wpływa na nasz mózg*, Gliwice 2013, p. 68.

in the reader than when browsing the Internet, which is connected with understanding the text written in the form of motionless but imaginative signs. What is important here is the individual interpretation of these signs and of the accompanying graphics by the subject of action.

When using "ready-made" information collected on the Internet, the user comes across already processed "pills" of information he/she is looking for. Search engines, though helpful in discovering the world, usually only give a fragmentary answer, a few words or sentences about what is needed at a given moment, usually not allowing one to grasp the whole picture or to find the essence of the information.

Communicating with others through text messages often boils down to writing a few words or a few simple sentences. These sequences are more and more often expressed in simple language, slang incomprehensible not only for foreigners.

The information on the monitor screen is meant to draw the attention of a fast-acting recipient. For this reason, the information environment must be properly designed to enable the user to move quickly within it. Another issue is the choice of the form of the message and its legibility. An information architect makes it easier to access by the following means:

- gathering different units of information,
- grouping units into useful categories,
- assigning easy names to the information, recognizable by most people,
- placing information in the places where it will be found most quickly.[41]

The most important goal of an information architect is to achieve customer satisfaction. The recipient is satisfied when he/she has quick access to information and the information itself is concise and easy to "digest". This means that the objectivity of information is usually translated into its simplified, non-textual superficial version, or even into mere catchy vulgarity.

In addition, the layout of the service is important for the customer, as well as navigation through it, e.g. a menu. This is particularly important when searching for various pieces of information of similar meaning or content. In this case, the recipient decides on the accuracy of the answer to the query him/herself. It is assumed that a correctly constructed piece of information performs its function best when it does not involve the user in thinking.[42]

[41] K. Lange-Sadzińska, *Architektura informacji w praktyce*, "Studies & Proceedings of Polish Association for Knowledge Management", 2011, no. 53, p. 99.

[42] D. Nojszewski, *Architektura informacji w kontekście budowy przestrzeni informacyjnej sieciowych systemów informacyjnych*, Wrocław 2004, http://www.zsi.pwr.wroc.pl/zsi/missi2004/pdf/Nojszewski%20Dariusz.pdf (accessed: 22.10.2019).

In this way, the recipient is slowly deprived of proficiency in the examined issues. The effect of such facilitation is the phenomenon of laziness of the Internet user's brain, which in consequence prevents him/her from deeper reflection on the content of information and its quality level.

The proper condition for effective learning that enables one to remain secure thanks to the consolidation of a given competence – i.e. the condition for fulfilling of what is required from a human being by *security culture* – is the continuous repetition (training of application) of obtained knowledge and related experience on the real physical level, not on the virtual level.

We should add to this condition the ability to correct our actions in the future, depending on whether any part or the entirety of our behaviour causes a defeat or guarantees a success. This training must be repeated over and over again in order to maintain a given value. Increasing precision and improving the flow of information saves the energy of the subject of action, and proper reaction in various situations leads faster to the intended goal.

If any experience proves to be good or at least sufficient for us, we strive to successfully renew it. If we are satisfied with the speed of obtaining information on the Internet and its accuracy, we will repeat the process of searching information on the Internet. It turns out that it seems to us that we no longer need deeper reflection in order to be effective. The active security subject must remember, however, that in this situation it is unavoidable that there is an abundance of information of a superficial nature, access to which is quick, but which is above all incomplete or untrue knowledge.

The knowledge gathered in virtual space is promoted as "instant knowledge". This is a very tempting idea, but often the price of this speed is the superficiality of information, which, what is worse, can be false, and the knowledge gained in such a way is at most shallow. Basing on such information, the amount of which additionally overloads the brain, distracts one from the depth of thinking. Only short-term memory is developing, which would normally, without the existence of digital information cacophony, play an important role in the transfer of information to long-term memory, so important to *security subjects*.

The excess of information and the question of security

Today, human does not suffer, as it used to be in the past, from lack of information, but from the overload of information. The location of the source of information and the qualitative selection thereof are of particular importance nowadays, also for security purposes. Nowadays, the existence of almost unlimited possibilities of manipulation with human consciousness creates significant threats. The flood of information is accompanied by the following negative social phenomena, which have a global impact:

- a disorderly, avalanche-like increase in the amount of information, the number of data and the volume of various knowledge resources,
- blurring of boundaries that existed between different spheres of information and knowledge;
- excessive uniformity of information and knowledge accompanying globalisation;
- informational and socio-cultural chaos, including confusion caused by spreading moral-ethical relativism, resulting in the quality, the quantity and the pace of changes in social reality getting out of human control.

The effect of the sheer volume of information accessible nowadays is a phenomenon referred to as information overload. It can lead to disturbances in the ability to properly assess the value of information. Information overload is understood as a kind of informational stress.

As Podgórski points out: "The tragedy of modernity consists in the fact that the speed of changes is greater than the awareness of many people".[43] The contemporary development of civilization which we are witnessing undoubtedly makes the everyday life of a human being easier in the technical dimension. On the other hand, however, the same development has its darker face, causing enormous difficulties, overload and problems in the existential dimension of human. The environment that human has created and continues to create is not only a proof of his/her ability, but can also be a source of danger, often difficult to predict.[44]

Moreover, the pressure of time, the shallowness of knowledge and thoughts, as well as information chaos, often cut off the possibility of absorbing into memory a long-term portion of proven, certain knowledge. Often, therefore, the user, as the subject of action, does not think about the

[43] R.A. Podgórski, *Socjologia mikrostruktury*, Bydgoszcz–Olsztyn 2008, p. 325.

[44] I. Wojnar, *Obszary humanistycznego zaniepokojenia*, "Przyszłość: Świat – Europa – Polska", 2014, no. 1, p. 18.

information obtained at a given stage of the search, but jumps to the next one. There is less and less analysis, focus on the content and substantive assessment of its value.

As mentioned earlier, the information obtained in this way is usually shallow. It is often not realized how high the required satisfactory level of knowledge on a given subject really is (and the realization thereof may affect the recipient's, and not only his/her, security). In addition, this way of obtaining information leads the user to run a new function, which is necessary for him/her in this rush; namely, he/she recklessly resolves to transfer his/her task of storing knowledge and data in his/her own brain to the network. But the *security subject*, especially at an early age, and his/her brain, should be subject to development processes rich in instructive challenges and stimuli. It is this development, and its level, that, in the future, will significantly affect the quality of the *security environment* of this *security subject*.

On the contrary, when the tools and sources of cognition are one-sided, due to the excessive use of the computer and the multimedia, the brain of this subject is to remember only this much:
(a) where the information can be found – and –
(b) how to ensure the availability of the source of electrical power.

Maintaining the prevalence of this developmentally limited system causes that the functioning of the brain becomes more and more shallow. In this case, the *security subject* no longer has a brain well prepared to carry out independent reflection on what he/she should store in his/her memory, which is independent of the computer – not necessarily accessible in need, e.g. at the time of danger. It is a question of a *security subject* (who is, at the same time, a multimedia recipient) being able to fight effectively for his/her values (this ability is the authors' own, alternative understanding of the notion of security) using his/her well-functioning and capacious long-term memory and his/her ability to reflect.

Let us stress that the user, due to his/her – not always fully conscious – need for intellectual independence, which cuts off the risks and threats posed by the so-called external control, is treated in these deliberations as a *security subject*. The level of *security culture* in an individual or in a human social group is determined by the level of quality (breadth and depth) of knowledge of the world possessed by these *security subjects*. Human, being a cognitive subject, shapes himself/herself as a *security subject* in his/her childhood, when he/she learns. Learning about reality is based on sensory experiences, including the sense of touch. *Homo sapiens hapticus* is a visual

and auditory learner, but he/she is also a kinaesthetic learner, which means that he/she gets to know the world and learns through non-virtual movement and touch.[45]

The dangers of over-exposure to digital media

A simple example of simultaneous work of body and mind is the first contact of a *security subject* with mathematics, i.e. counting on fingers. Brain development requires early, simple, kinaesthetic and non-virtual[46] forms of knowledge acquisition, without which it is difficult to develop the satisfactory level of abstract thinking.[47] Scientific experiments have confirmed that functional patterns of activation in the human brain become established as conceptual structures only when the assimilation of knowledge is accompanied by real – that is to say, non-virtual, manual – activities. Cognition via a computer mouse implies deterioration in the ability to reflect on this cognition itself.[48]

The correctness of the above statement is also proven by the fact that the learning and assimilation of the components of the alphabet, i.e. letters, by the subject works best when it is carried out by independent handwriting of letters, not with the use of computer keyboard,[49] which later also affects the level of reading skills.

A child can learn to use a computer or television relatively quickly, but as a *security subject*, it is not yet adapted to receive the excess of stimuli flowing from these devices and his/her eye should not see the moving images at least until the age of three, if we do not want to "injure" this organ. A child's eye should learn three-dimensional vision. Only later, preferably not before the age of four, can he/she use the media, but only under the strict supervision of a parent who interprets everything that happens on the screen.

Another aspect of media abuse is the use of media in the bedroom and leaving it there rather than in the living room. This allows for too frequent,

[45] Cf. M. Grunwald, *Homo hapticus…*, *op. cit.*

[46] See: *Wirtual. Czy nowy wspaniały świat?*, K. Korab (ed.), Warszawa 2010.

[47] M. Spitzer, *Cyfrowa demencja. W jaki sposób pozbawiamy rozumu siebie i swoje dzieci*, Słupsk 2013, p. 147.

[48] *Ibidem*, p. 157.

[49] M. Kiefer, E. J. Sim, B. Herrnberger, J. Grothe, K. Hoenig, *The sound of concepts: four markers for a link between auditory and conceptual brain systems*, "The Journal of Neuroscience", 2008, 28(47), pp. 12224-12230, https://doi.org/10.1523/JNEUROSCI.3579-08.2008.

unstructured use of the Internet by a young, newly psychophysically formed *security subject*, leading, among other things, to shortening the time of his/her sleep and inappropriate habits from the point of view of the "hygiene" of multimedia use. Moreover, children who have more friends in the real social world sleep better and longer.[50] Parents may believe in good faith that e.g. computer games belong to the subculture of young people, and resignation from them may have a negative impact on contacts with peers. Children are bought games that give them an attractive thrill – which can be achieved by showing violence. It is believed that this supports young people's social competences and protects them from alienation. Science, however, denies this position.

Research on teenage personality development has shown that an hour spent in front of a computer screen or monitor increases the risk of deterioration in the relationship with parents by up to a dozen or so percent. In addition, it is accompanied by the weakening of bonds with peers and friends. The human brain works most effectively in direct interaction with other people and learns most from direct exchanges of views and experiences in a social group. In addition, the human tendency to imitate catalyses the process of acquiring new skills. The brain then activates structures called mirror neurons.[51]

This mechanism is clearly visible in young children, who are learning and willing to imitate the behaviour of adults. This type of interaction cannot occur fully via the computer.

The consequences of Internet addictions (already existing in the social world) is the progressive degradation in an addicted *security subject* of, among others, such *security culture* factors as the ability to concentrate, family bonds, parental influence, social activity, real friendships (not only virtual ones) and entering into direct interpersonal relations instead of engaging in illusory virtual contacts, having passion or hobbies, having the potential of willpower, regular rhythm of activity and sleep, taking care of everyday learning, regularity of eating, openness and empathy prevailing over egocentrism and egoism, well-established awareness of the shape of one's own identity, intellectual fitness, ordering the needs of the sexual sphere,

[50] R. Pea, C. Nass, L. Meheula, M. Rance, A. Kumar, H. Bamford, M. Nass, A. Simha, B. Stillerman, S. Yang, M. Zhou, *Media use, face-to-face communication, media multitasking, and social well-being among 8- to 12-year-old girls*, "Developmental Psychology", 2012, no. 48(2), https://doi.org/10.1037/a0027030, p. 327.

[51] M. Żylińska, *Neurodydaktyka. Nauczanie i uczenie się przyjazne mózgowi*, Toruń 2013.

self-control – also in terms of time spent surfing the net, natural care for personal health and hygiene, or self-fulfilment thanks to a good position in the workplace.[52] An addictive factor does not have to be a substance: certain behavioural patterns may also become addictive.[53]

Civilisational progress and the importance of *personal security*

The currently observed progress means that a person can possess what he/she wants and, what is more, to be what he/she wants. It can be said that consumerism, apart from the fact that it undoubtedly plays a key role in creating social divisions, also seems to play such a role in creating one's own identity and introducing the mechanism of illusion and denial, thus supplanting the rational approach with magical and wishful thinking, which can be compared to dependence on substances such as alcohol.[54] Consumption is considered a value to be pursued in the modern world. This is particularly evident in the behaviour of young people, who are accustomed to the ideology of consumerism from an early age, which is widespread, for example, in the media. But not everyone can afford all the amenities of today's world. The sense of meaninglessness and the conviction of one's lower position is undoubtedly a serious psychological problem in modern times.

The contemporary world undoubtedly cares about respect for freedom, choices, otherness, and the emphasis on the subjectivity of the individual. On the other hand, however, it is an unpredictable world in which the individual often feels lonely and lost. Bauman writes: "We can imagine modernity (which in the final analysis is a state of compulsive, obsessive and addictive modernization, meaning »to make things better than they are today«) as a sword constantly turned against the existing reality".[55]

However, in the face of many positive developments, harmful phenomena do not disappear, and many of them are still developing. Promoting the idea of "you only live once" and the constant changes in realities, to which it is sometimes difficult to adapt, makes the contemporary world bring a number of burdens for the individual. The speed of recent progress is often

[52] G. Kiedrowicz, *Zagrożenia dla edukacji wspomaganej technologią informacyjną*, "Gazeta-IT", http://gazeta it.pl/en/education/5065 (accessed 22.10.2019).

[53] M.R. Jabłońska, *Człowiek w cyberprzestrzeni. Wprowadzenie do psychologii Internetu*, Łódź 2018, p. 134.

[54] J. Mellibruda, *Psycho-bio-społeczna koncepcja uzależnienia od alkoholu*, "Alkoholizm i Narkomania", 3(28), pp. 277–306.

[55] Z. Bauman, D. Lyon, *Płynna inwigilacja. Rozmowy*, Kraków 2013, p. 139.

the cause of many social problems. The fact that the topic of loneliness was one of the most important topics of the last World Economic Forum summit in Davos, which showed that in many Western civilizations more than 30% of the society suffers from the lasting effects of loneliness, proves it. The increasing loneliness of young people, too, generates a huge cost for the global economy. This can also be seen in Poland, for example in the growing number of depression cases. In 2018 even the Supreme Chamber of Control became interested in this phenomenon when it turned out that the number of suicides in our country is higher than the number of car accident victims.[56]

This is why personal security is so important. Governments are developing offensive capabilities in cyberspace and the number of cyberattacks by state actors on civilians and critical infrastructure is increasing. The number of cyberattacks is increasing exponentially, and new threats are still appearing. However, this is only one important aspect. The perception of cybersecurity today is almost exclusively "hard cyber". However, it is worthwhile to implement a reflection on security in the humanistic sense, as an attribute of human, into these considerations.

As Drabik points out, "a secure being is a humanistic, cultural and, finally, abstract being, which elevates the meaning of the concept of security beyond the area of biology and behavioural processes. Biological persistence alone does not fill the meaningful charge hidden behind the collection of designations of the concept of security. Cultural provenance points to its abstract context, linked not only to human rationality but also to the ability to create abstract concepts and artefacts".[57]

Grabińska, in her article *Zagrożenia bezpieczeństwa społecznego w ideologii transhumanizmu*,[58] describes personal security as "the security of a person in his/her subjective perception in relation to structural security, but not only as a result of objective minimization of structural threats". Personal security is therefore not the same as *personal safety*, as defined in psychology. And shaping the sense of personal security in every human being is the basis of security in all its other dimensions.

[56] Z. Dzik, *Człowiek i sztuczna inteligencja: wybory odpowiedzialności. O wpływie technologii na człowieka*, "Newsweek Psychologia", no. 2/2019, pp. 102–106.

[57] K. Drabik, *Dekonstrukcyjne…*, *op. cit.*, p. 44.

[58] T. Grabińska, *Zagrożenia bezpieczeństwa społecznego w ideologii transhumanizmu*, "Kultura Bezpieczeństwa. Nauka – Praktyka – Refleksje", 2015, no. 18, pp. 52–73.

Fighting modern threats in practice: cybersecurity in Poland

Ensuring information security is a challenge for all entities creating a national cybersecurity system, i.e. economic entities providing services using ICT systems, users of cyberspace, public authorities, as well as specialised entities dealing with ICT security in the operational sphere. This is all the more important because Poland is closely connected with other countries through international cooperation within organizations such as the EU, NATO, UN or OSCE. The Internet has become a tool to influence the behaviour of social groups, as well as influence in the political sphere, and this is why Poland has introduced the *National Framework of Cybersecurity Policy of the Republic of Poland for 2017–2022*.[59] This document is a continuation of actions taken in the past by the government administration aimed at increasing the level of security in the Polish cyberspace, including the *Policy for the Protection of the Cyberspace of the Republic of Poland* adopted by the government in 2013.[60] The National Framework of Cybersecurity Policy indicates, in particular:

- ICT security objectives,
- the main actors involved in the implementation of national ICT security policy frameworks,
- a governance framework to achieve the objectives of the national ICT security policy framework,
- the need to prevent and respond to incidents and to restore the normal state disrupted by incidents, which includes cooperation between the public and private sectors,
- the approach to risk assessment,
- orientations for educational, information and training programmes on cybersecurity,

[59] Ministerstwo Cyfryzacji, *Krajowe Ramy Polityki Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017–2022*, Warszawa 2017.
The document was prepared by a group consisting of representatives of the following ministries: Digitalization, National Defence, Internal Affairs and Administration, as well as representatives of the Internal Security Agency, the Government Security Centre and the National Security Bureau.

[60] Rzeczpospolita Polska, Ministerstwo Administracji i Cyfryzacji, Agencja Bezpieczeństwa Wewnętrznego, *Polityka Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej*, Warszawa, 25 June 2013.

- actions relating to research and development plans in the field of ICT security,
- the approach to international cooperation on cyber security.[61]

The National Framework of Cybersecurity Policy introduced by a resolution of the Council of Ministers has a direct impact on government administration entities, and an indirect impact, following the adoption of universal law regulations at the initiative of the Council of Ministers, on other entities of public authority, entrepreneurs and citizens.

The condition for the proper functioning of the national cybersecurity system in the *national security system* will be the clarification of the nature of the interrelations between the various stakeholders of this system. It is about relations and interdependencies connecting such different elements as authorities and entities responsible for: national security, internal security, public order, and, finally, for the fundamental sphere of the personal dimension of security, which has a humanistic core – that is, education, development and raising the self-awareness of *security subjects*.

Conclusion

To conclude, for a researcher in security sciences, i.e. the study of threats and security, among *security environments* to be investigated there is cybersecurity, in which the process of communication is an important component of the power manifested by the aforementioned *second stream of energy* of *security culture*, referring to the potentials of human social communities. At the end of this study, it is worth quoting the notion of *liquid modernity* conceived by Bauman, which he defined as a reality in which traditional norms and traditional social roles are lost.[62] This is due to the constant changes that we are witnessing. They require continuous verification of the knowledge and skills of a human being. Moreover, constant progress means that there is often no room for reflection. It is also not difficult to change or lose one's identity.

In literature there is a concept of a *human gap*. It is a dissonance between the complexity of social reality and human's ability to cope with it. A large amount of changes, stimuli and information makes it impossible for everyone to keep up with the development. It is then that the human gap is

[61] Ministerstwo Cyfryzacji, *Krajowe Ramy…*, *op. cit.*

[62] See: Z. Bauman, *Płynna nowoczesność*, Kraków 2000.

created, which is the dissonance between the growing progress and people's ability to cope with it. This is due to the fact that the increase in human-made innovation is not matched by the increase in human skills.[63] Thus, the chaos of consciousness is created, which requires a struggle for the human and the human security in every dimension. We will ask why? Because today the human condition is often reduced to consumption and humans live in a culture of excessive choice. One can see that people are lost, increasingly lonely and deprived of insight into themselves, or self-awareness.

As Grabińska points out, "communities living in the [cultural] circle of personalist ethics are generally poorer, but paradoxically they live in a greater sense of security. That is why the constant pursuit of ever-increasing wealth and power is not their goal. However, societies living within the circle of utilitarian ethics, internally antagonized and atomized because of the desire and specific compulsion to achieve the same individual good (...) seem to have a lesser sense of security, which can only increase the amount of material goods possessed, i.e. wealth and domination over others".[64]

References

1. Antonsen S., *Safety Culture: Theory, Method and Improvement*, Burlington 2009.
2. Batorowska H., *Kultura bezpieczeństwa informacyjnego*, "Edukacja – Technika – Informatyka", 2018, no. 1/23/2018, pp. 92–100, https://doi.org/10.15584/eti.2018.1.11, https://repozytorium.ur.edu.pl/bitstream/handle/item/3957/11%20batorowska-kultura%20bezpieczeństwa.pdf?sequence=1sAllowed=y (accessed 22.10.2019).
3. Bauman Z., *Płynna nowoczesność*, Kraków 2000.
4. Bauman Z., Lyon D., *Płynna inwigilacja. Rozmowy*, Kraków 2013.
5. Bell D., *The Third Technological Revolution and its Possible Socioeconomic Consequences*, "Dissent", 1989, Spring, pp. 164–167.
6. *Biała Księga Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej*, Warszawa 2013.
7. Botkin J.W., Elmandjra M., Malitza M., *Uczyć się – bez granic*, Warszawa 1982.

[63] J.W. Botkin, M. Elmandjra, M. Malitza, *Uczyć się – bez granic*, Warszawa 1982, pp. 47–48.

[64] T. Grabińska, *Etyka…*, *op. cit.*, p. 15.

8. Bush V., *As we may think*, „The Atlantic", 1945, http://www.theatlantic.com/magazine/archi-ve/1945/07/as-we-may-think/303881/ (accessed 22.10.2019).
9. Buzan B., *New Patterns of Global Security in the Twenty-First Century*, „International Affairs", 1991, vol. 67, no. 3, pp. 431–451.
10. Carr N., *Płytki umysł. Jak Internet wpływa na nasz mózg*, Gliwice 2013.
11. Castells M., *Społeczeństwo sieci*, Warszawa 2008.
12. Cieślarczyk M., *Kultura bezpieczeństwa i obronności*, Siedlce 2011.
13. Doktorowicz K., *Europejski model społeczeństwa informacyjnego. Polityczna strategia Unii Europejskiej w kontekście globalnych problemów wieku informacji*, Katowice 2005.
14. Drabik K., *Dekonstrukcyjne i konstrukcyjne funkcje zagrożeń w kształtowaniu bezpieczeństwa personalnego*, [in:] *Problemy bezpieczeństwa i zarządzania kryzysowego*, M.R. Gogolin (ed.), vol. II, Bydgoszcz 2019, pp. 44–55.
15. Dzik Z., *Człowiek i sztuczna inteligencja: wybory odpowiedzialności. O wpływie technologii na człowieka*, "Newsweek Psychologia", no. 2/2019, pp. 102–106.
16. Garud R., *The Social Construction of Technological Reality*, London 2018.
17. Goban-Klas T., Sienkiewicz P., *Społeczeństwo informacyjne: szanse, zagrożenia, wyzwania*, Kraków 1999.
18. Grabińska T., *Etyka a bezpieczeństwo personalne*, Wrocław 2013.
19. Grabińska T., *Zagrożenia bezpieczeństwa społecznego w ideologii transhumanizmu*, "Kultura Bezpieczeństwa. Nauka – Praktyka – Refleksje", 2015, no. 18, pp. 52–73.
20. Grunwald M., *Homo hapticus. Dlaczego nie możemy żyć bez zmysłu dotyku*, Kraków 2019.
21. Jabłońska M.R., *Człowiek w cyberprzestrzeni. Wprowadzenie do psychologii Internetu*, Łódź 2018.
22. Jarmoszko S., *Status kultury strategicznej w kontekście badania i kreowania kultury bezpieczeństwa*, [in:] *Elementy teorii i praktyki transdyscyplinarnych problemów bezpieczeństwa*, A. Filipek (red.), vol. II, Siedlce 2014, pp. 289–308.
23. Kaebnick G.E., *Humans in Nature: The World As We Find It and the World As We Create It*, New York 2013.
24. Kiedrowicz G., *Zagrożenia dla edukacji wspomaganej technologią informacyjną*, "Gazeta-IT", http://gazeta it.pl/en/education/5065 (accessed 22.10.2019).

25. Kiefer M., Sim E.J., Herrnberger B., Grothe J., Hoenig K., *The sound of concepts: four markers for a link between auditory and conceptual brain systems*, "The Journal of Neuroscience", 2008, 28(47), pp. 12224–12230, https://doi.org/10.1523/JNEUROSCI.3579-08.2008.
26. Kitler W., *Transdyscyplinarność badań w naukach o bezpieczeństwie i w naukach o obronności*, [in:] *Metodologiczne i dydaktyczne aspekty bezpieczeństwa narodowego*, W. Kitler, T. Kośmider (eds), Warszawa 2015, pp. 159–177.
27. Korus J., *Mglista przyszłość naszych wspomnień*, "Newsweek. Tajemnice przyszłości", 1/2019, pp. 102–107.
28. Kowalczyk M., *Cyfrowe Państwo. Uwarunkowania i perspektywy*, Warszawa 2019.
29. Kroeber A.L., *The Nature of Culture*, Chicago 1952.
30. Krzysztofek K., *Rdzeń kultury a cywilizacje*, "Transformacje", 1995/1996, no. 3/4, pp. 151–160.
31. Kubiak M., *Filozofia bezpieczeństwa personalnego i strukturalnego*: *tradycja – współczesność – nowe wyzwania*, Siedlce 2007.
32. Lange-Sadzińska K., *Architektura informacji w praktyce*, "Studies & Proceedings of Polish Association for Knowledge Management", 2011, no. 53, pp. 93–103.
33. Mellibruda J., *Psycho-bio-społeczna koncepcją uzależnienia od alkoholu*, "Alkoholizm i Narkomania", 3(28), pp. 277–306.
34. Ministerstwo Cyfryzacji, *Krajowe Ramy Polityki Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017–2022*, Warszawa 2017.
35. Nojszewski D., *Architektura informacji w kontekście budowy przestrzeni informacyjnej sieciowych systemów informacyjnych*, Wrocław 2004, http://www.zsi.pwr.wroc.pl/zsi/missi2004/pdf/Nojszewski%20Dariusz.pdf (accessed: 22.10.2019).
36. Nowina-Konopka M., *Istota i rozwój społeczeństwa informacyjnego*, [in:] T. Białobłocki, J. Moroz, M. Nowina-Konopka, L. Zacher, *Społeczeństwo informacyjne. Istota, rozwój, wyzwania*, Warszawa 2006, pp. 13–59.
37. Pea R., Nass C., Meheula L., Rance M., Kumar A., Bamford H., Nass M., Simha A., Stillerman B., Yang S., Zhou M., *Media use, face-to-face communication, media multitasking, and social well-being among 8- to 12-year-old girls*, "Developmental Psychology", 2012, no. 48(2), pp. 327–336, https://doi.org/10.1037/a0027030.

38. Pidgeon N., *Safety culture and risk management in organizations*, "Journal of Cross-Cultural Psychology", 1991, no. 22, pp. 129–140, https://doi.org/10.1177/0022022191221009.
39. Piwowarski J., *Nauki o bezpieczeństwie. Kultura bezpieczeństwa i redefinicja środowiska bezpieczeństwa,* Warszawa 2020.
40. Piwowarski J., *Społeczeństwo informacyjne a kultura bezpieczeństwa*, "Zeszyt Naukowy WSBPI »Apeiron« w Krakowie", 2011, no. 6, pp. 161–174.
41. Piwowarski J., *The security (culture) rhombus. Redefining security environment*, "Kultura Bezpieczeństwa", 2019, no. 34, 141–154, https://doi.org/10.5604/01.3001.0013.5190.
42. Piwowarski J., *Three pillars of security culture*, "Kultura Bezpieczeństwa. Nauka – Praktyka – Refleksje", 2018, no. 29(29), pp. 22–32, https://doi.org/10.24356/KB/19/2.
43. Podgórski R.A., *Socjologia mikrostruktury*, Bydgoszcz–Olsztyn 2008.
44. Rzeczpospolita Polska, Ministerstwo Administracji i Cyfryzacji, Agencja Bezpieczeństwa Wewnętrznego, *Polityka Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej*, Warszawa, 25 June 2013.
45. Schütz A., *The Phenomenology of the Social World*, Evanston 1997.
46. Searle J.R., *The Construction of Social Reality*, New York 1996.
47. Spitzer M., *Cyfrowa demencja. W jaki sposób pozbawiamy rozumu siebie i swoje dzieci*, Słupsk 2013.
48. Toffler A., *Szok przyszłości*, Warszawa 1970.
49. Turing A., *Computing Machinery and Intelligence*, "Mind", vol. LIX, no. 236, October 1950, pp. 433–460, http://web.archive.org/web/20110726153108/http://orium.homelinux.org/paper/turingai.pdf (accessed 22.10.2019).
50. Vogl C.H., *The Art of Community: Seven Principles for Belonging*, Oakland 2016.
51. Webster F., *Theories of the Information Society*, London–New York 2002.
52. *Wirtual. Czy nowy wspaniały świat?*, K. Korab (ed.), Warszawa 2010.
53. Wojnar I., *Obszary humanistycznego zaniepokojenia*, "Przyszłość: Świat – Europa – Polska", 2014, no. 1, pp. 15–24.
54. Zohar D., *Safety climate in industrial organizations: Theoretical and applied implications*, "Journal of Applied Psychology", 1980, no. 65(1), pp. 96–102, https://doi.org/10.1037/0021-9010.65.1.96.
55. Żylińska M., *Neurodydaktyka. Nauczanie i uczenie się przyjazne mózgowi*, Toruń 2013.

CITE THIS ARTICLE AS

J. Piwowarski, R. Rodasik, *Prolegomena for studying security culture in cybersociety,* [in:] *Security in Central and Eastern Europe: Cyberspace, Police, Prisons, Transport, Addictions, the Media. Proceedings from the Conference XLIV CICA: "Security in Europe" – 12th Security Forum Krakow, 5–7 June 2018, Kraków, Poland*, Krakow 2020, pp. 20–49, https://doi.org/10.24356/proceedings2018/1.

UNIFORMED SERVICES AND NATIONAL SECURITY IN THE CZECH REPUBLIC

**SECURITY IN CENTRAL AND EASTERN EUROPE:
CYBERSPACE, POLICE, PRISONS, TRANSPORT, ADDICTIONS, THE MEDIA**
Proceedings from the Conference
XLIV CICA: "Security in Europe" – 12th Security Forum Krakow
5–7 June 2018, Kraków, Poland
2020 (52–64); https://doi.org/10.24356/proceedings2018/2

Fuzzy Problems in Security Management: New Threats and the Importance of Tacit Knowledge in the Police of the Czech Republic

Dana Junková*
Milan Kný**

ABSTRACT

Although findings in security sciences expand human knowledge about threats, the implementation of this knowledge is becoming increasingly difficult in the contemporary turbulent environment with its uncertainty,

* Ing. Dana Junková, Ph.D., The Police Academy of the Czech Republic in Prague, Prague, Czech Republic; correspondence address: The Police Academy of the Czech Republic in Prague, Lhotecka 559/7, 143 01 Praha 4, Czech Republic; email: junkova@polac.cz
** Ing. Milan Kný, CSc., The Police Academy of the Czech Republic in Prague, Prague, Czech Republic.

instability, ambiquity and complexity. The fuzzy[1] problems of the current security situation in the Czech Republic – when criminal activity becomes more sophisticated than in the past, when the structure of this activity changes and the severity of crimes against society increases[2] – must be seen as latent and potential threats of the near and distant future. These facts, combined with higher latency of crime, place increased demands on the search for criminal activities and the overall work of the officers of the Police of the Czech Republic, their education and knowledge. Among the tools and components of security management, there are knowledge management and effective knowledge transfer, because it is not enough to gain and keep knowledge; it is also necessary to share it horizontally and vertically. The contribution presents the results of the pilot survey on the methods of transferring tacit knowledge in the Police of the Czech Republic on the level of top management. It also supplements the concept of the organizational approach to the internal and external security of the state.

ARTICLE INFO

Article history
Received: 10.09.2018 Accepted: 4.04.2019

Keywords
fuzzy problem, knowledge, latent threat, hidden threat, security management

Introduction

Safety is one of the basic needs of all citizens and security in a democratic society belongs to the fundamental values and priority social goals. However, in the current global society, which is exposed to turbulent conditions and constant change, the nature of which is often discontinuous, safety is increasingly threatened. The fuzzy problems of the current security situation must be seen as latent and potential threats of the near and distant future. In contrast to more explicit security problems, such as terrorism, undesirable immigration and organized crime, or money laundering and corruption, there are also clusters of more elusive economic, social and political risks which, although their occurence is less probable than that of the previously

[1] Fuzzy – in English: 'hazy, vague, indeterminate'.

[2] In economic area for example: moral hazard or rent-seeking.

mentioned risks, can also bring about considerable dangers. It is therefore essential for the theory and practice of security management to be able to react quickly and accordingly to actual changes. The article is a contribution to security sciences, and it emphasises the growing importance of the tasks of strategic security management, knowledge management, and the multidisciplinary approach to security.

Methodological approach

Table 1 below presents an extended concept of the internal and external security of the state, which has been investigated in the authors' earlier work.[3]

Table 1. The conceptual field of the internal and external security of the state

	INTERNAL AND EXTERNAL SECURITY OF THE STATE			
	1st dimension Ideals, values, mental wealth of man	**2nd dimension** Social influences of the organisation, legal systems	**3rd dimension** Material aspects of the human existence	**4th dimension** Space, including cybernetic space
State forms of protection: • Police • Army	• Internal security • External security			
Private forms of protection:	Private/business security services			
The time aspect:	Past – present – future			

Source: own editing based on Cieślarczyk,[4] Sheptycki,[5] Kný and Junková[6]

[3] M. Kný, D. Junková, *Vlivové faktory bezpečnostního managementu*, "Kultura Bezpieczeństwa. Nauka – Praktyka – Refleksje", 2017, no. 28, pp. 124–135, https://doi.org/10.24356/KB/28/5.

[4] In: J. Piwowarski, *Three Pillars of Security Culture*, "Security Dimensions. International and National Studies", 2015, no. 14, pp. 10–16, https://doi.org/10.5604/01.3001.0012.5891.

[5] *Transnational Policing Issues*, J. Sheptycki (ed.), London 2000, p. 11, [qtd. in:] B. Bradford, B. Jauregui, I. Loader, J. Steinberg, *Global Policing*, London 2016.

[6] M. Kný, D. Junková, *Vlivové…*, *op. cit.*

It distinguishes between four dimensions of security (the first: ideals, values and the mental wealth of man; the second: social influences, organizations and legal systems; the third: the material aspects of human existence; and the fourth: space, including cybernetic space[7]) and it takes into consideration the necessity of guaranteeing security to security subjects in real time.

While the military is the guarantor of external security, the police ensure internal security. The actual global security situation is characterized by the danger of new specific phenomena and risks that have a significant potential for endangering the internal security of the Czech Republic. At the same time, some existing risks may escalate quickly and easily. Among external influences with the potential impact on the level of internal security of the Czech Republic, there are:[8] worldwide threat of terrorism, radical growth of legal and illegal migration, radicalization and increase of extremist forces, internal security crisis and political crisis in Ukraine, transnational cybercrime, growth of drug distribution at international level, threat of hybrid war, and non-antropogenic threats (climate change).

In practice, the exact boundaries between the four dimensions of internal and external security are often vague. The protective function is an essential function of every state in all moments of its existence. At the same time, however, the protection of fundamental rights and freedoms of individuals often calls for restrictions on the rights of other persons. Here it is necessary to ensure that the police force unconditionally adheres to respect for the human dignity of the individual and restrict human rights only on the basis of the law, and to the extent that is strictly necessary. Without sufficient staff, finance, materials and knowledge, the police force can easily threaten the fundamental human rights of all the subjects that the armed forces protect. The principle says that as the complexity of the system increases, the observer's ability to formulate exact and important statements decreases up to a certain threshold, beyond which precision and importance are mutually excluding characteristics. "In fuzzy theory words,

[7] Cybernetic space: the digital environment allowing information to be created, processed and exchanged by means of information systems, electronic communications services and networks. Source: P. Jirásek, L. Novák, J. Požár, *Cyber security glossary*, Prague 2015, p. 70.

[8] *Koncepce rozvoje Policie České republiky do roku 2020 (aktualizace 2017)* [Concept of the development of the Police of the Czech Republic up to 2020 (updated in 2017)], http://www.ceska-justice.cz/wp-content/uploads/2017/04/Koncepce-rozvoje-Policie.pdf (accessed 26.06.2018), pp. 16–17.

the principle can be expressed as follows: The closer the problem is to the real world, the more fuzzy it becomes".[9]

What can and what cannot be seen

Security situation can be documented by monitoring the long-term development of crime in a certain area. Since 2008, registered crime has decreased not only in the Czech Republic,[10] but also in Europe and in the world in general (with the exception of the South American states). Property crime and robbery show the highest decrease. However, the number of 1) **economic crimes** and 2) **cybercrimes** has increased.[11]

Re 1) In the Czech Republic **economic crime** represents only 10% of the total crime, but the damage caused by this type of crime in the period 2006–2015 is around 73% of the total recorded damages. "The most important subject damaged by serious economic crime is, in the long term, the Czech state. In its serious form, at present, economic crime is the most dangerous element threatening the proper functioning of the economic processes of democratic society in the Czech Republic".[12] There is a non-negligible risk of "rent-seeking" by parasiting the public finances and, in particular, there is a risk of a vicious circle, where concentration of economic power leads to political power, and political power allows a further increase of economic power which, in the long-term, may breach the market system and weaken democratic institutions. The higher latency of crime places increased demands on the search for crime. The problem is also the reduced criminal sensitivity, where society ceases to perceive some forms of criminality as "criminal". As a result, such an act is less reported (e.g. criminality against public order, or tax crime).

[9] P. Vysoký, *Fuzzy logics – fashion or a paradigm change?*, "Vesmír", 1994, no. 6, p. 73, https://vesmir.cz/cz/casopis/archiv-casopisu/1994/cislo-6/fuzzy-logika-moda-ci-zmena-paradigmatu.html (accessed 05.04.2018).

[10] According to *Concept of the development of the Police of the Czech Republic up to 2020*, in 2006 there were 336,446 incidents and 145,771 were cleared up in the Czech Republic, in 2015 247,628 incidents were registered and 126,083 were cleared up. In: *Koncepce…*, *op. cit.*

[11] *Koncepce…*, *op. cit.*

[12] *Ibidem*.

Re 2) **Cybercrime**[13] is a highly sophisticated crime committed using IT technology that creates cyberspace[14] and its virtual world, that is parallel to real space. It may involve fraudulent activities, intellectual property rights violations, virtual identity theft, so-called phishing attacks, unauthorized access to accounts, theft of economic data and running electronic communications, attacks aimed at destabilizing data communication, spreading child pornography, extremism, extortion, threats, dangerous persecution, etc. "Cybercrime activity causes damage to a great number of people and the relative anonymity of the offenders is typical".[15] There is a risk that present unobtrusive socio-pathological activities, such as behaviour on social networks, the presentation of propaganda or advertisement, may turn into new threats in the future. The cases of new security incidents in the "digital world" are growing and the legislation for their non-acceptance and punishment comes subsequently. Determining the origin of the offender and protection against these incidents are also problematic.

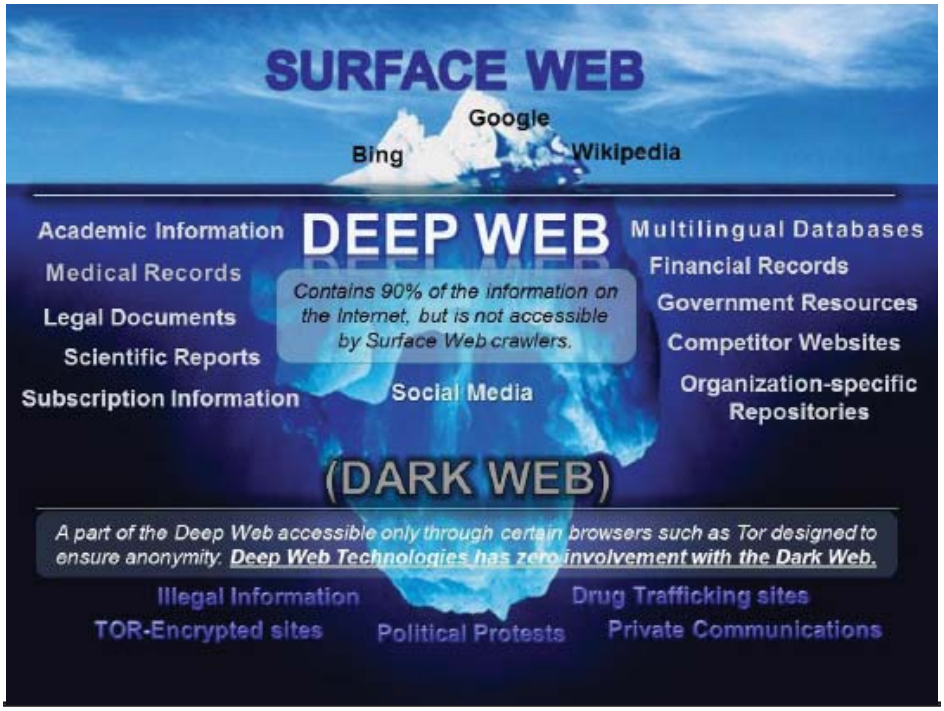
In Figure 1 below, the cyberspace display divides the imaginary cyberspace glacier into the visible and invisible parts. The standard user, using normal means, moves in the visible part, in the so-called Surface Web, which is only about 4% of cyberspace. Deep Web and Dark Web account for 96% of cyberspace content and are invisible to the common user.

[13] J. Kolouch, *CyberCrime*, Prague 2016, pp. 42–49.

[14] *Idem*, *Kyberprostor*, Praha 2016, http://www.teorieib.cz/pbi/files/281-Kyberprostor-Kolouch.pdf (accessed 23.06.2018).

[15] K. Kolářová, *Kyberkriminalita v Česku vzrostla za sedm let téměř čtyřnásobně*, "Lidovky.cz", http://ceskapozice.lidovky.cz/kyberkriminalita-v-cesku-vzrostla-za-sedm-let-temer-ctyrnasobne-phi-/tema.aspx?c=A180515_171751_pozice-tema_lube (accessed 29.06.2018).

Fig. 1. Cyberspace display



Source: *The "Deep Web" is Not All Dark*, https://i2.wp.com/www.deepwebtech.com/wp-content/uploads/DeepvsDarkIceberg.jpg (accessed 29.06.2018).

Security management, as well as economics and other scientific disciplines, must deal not only with the facts that are clear from the very beginning, but also, even more intensively, with those that are not evident at the first sight.

The importance of the elements and relations of the security system that "cannot be seen" (such as the rule of law and the effectiveness of law enforcement, the activities of police forces, the trust of the population in the police as regards dealing with crime, the moral and social climate, the political system, or the economic situation in society) is increasing.

Tacit knowledge as one of the conditions of effective police work

"Police work is a long-term activity characterized by a considerable time-consuming training, and a long-term return of investments in personnel

development".[16] At the same time, tacit, implicit and explicit knowledge is vitally important to solving crimes.

Knowledge is a constantly changing system that contains interactions between the inner and the outer environment of its owner. Veber states that knowledge can be defined through the notion of information: "knowledge = information + x",[17] where x represents the content with which a new piece of information in the human brain interacts, that is, one's previous knowledge and skills, experience, mental models, etc.

Professional literature lists various kinds of knowledge: formal and informal, soft and hard, know-how and know-what, transitive and source-based, individual and collective. However, in most cases professional literature is supported by Polanyi's classification[18] which distinguishes between two dimensions of knowledge: explicit (expressed, recorded) and tacit (hidden, subconscious).

Table 2. Characteristics of explicit and tacit knowledge

Tacit knowledge	**Explicit knowledge**
It cannot be expressed in a recordable form	It is already expressed and accessible
Subjective	Objective
Personal	Interpersonal
It relates to a specific context	It is not related to a specific context
Hard to share	Easily shared

Source: D. Hislop, *Knowledge management in organizations: a critical introduction*, Oxford 2013, p. 21.

Tacit (subconscious) knowledge is often hidden compared to explicit knowledge, and is highly personal. Therefore, it is very difficult to formally express and share it. Sternberg notes that tacit knowledge "is based on prac-

[16] *Koncepce…*, *op. cit.*, p. 24.

[17] J. Veber *et al.*, *Management. Základy – moderní manažerské přístupy – výkonnost a prosperita*, Praha 2009, p. 589.

[18] M. Polayi, *Personal Knowledge: Towards a Post-Critical Philosophy*, Chicago 1958, [qtd. in:] J.L. Rice, B.S. Rice, *The Applicability of the SECI model to Multi-organisational endeavours: an integrative review*, "International Journal of Organisational Behaviour", 2009, vol. 9, no. 8, p. 671.

tical intelligence rather than on intellectual or academic knowledge".[19] Švec considers tacit knowledge as the part of expert knowledge "the development of which can be stimulated by methods that stimulate the thinking and self-reflection of the subject".[20] It is generally stated that tacit knowledge is of a procedural nature. Mladkova[21] states that Western experts (USA, Europe) perceive knowledge as primarily explicit and experts from Eastern (Asian) countries (China, Japan) as primarily tacit.

Also the method of transferring knowledge differs according to whether it is explicit or tacit. Explicit knowledge is easier and better transferable than tacit knowledge. Explicit knowledge requires formal transfer methods in which documents, data and other sources are caught and saved in a particular format on a specific facility that can be accessed by other potential users (manuals, books, databases, information systems, etc.). For transferring tacit knowledge, which, by its nature, is more complicated, personal contact is very important. Personal contact allows to pass the context of the knowledge, which includes a certain life experience, specific historical circumstances, the know-how of the knowledge-owner, etc.

The methods of transferring tacit knowledge, according to Krisnaveni and Sujatha,[22] include: active learning, blogs, brainstorming, e-learning and e-cooperation, meetings, mentoring, metaphors and analogies, working groups, case studies, socialization and outsourcing, social networks, questioning techniques and apprenticeship.

Police officers are considered by experts to be knowledge workers and police work is recognized as "knowledge-based." The quality of police knowledge and its effective management is a key area of police practice.[23]

Some of the turbulent phenomena show first in the form of weak signals and symptoms, which can be detected at a stage when there is no immediate

[19] R. Sternberg, *What Do We Know About Tacit Knowledge? Making the Tacit Become Explicit*, London 1999, [qtd. in:] J.L. Rice, B.S. Rice, *The Applicability…*, *op. cit.*, p. 674.

[20] V. Švec, *What Do We Know About Tacit Knowledge? Development of managers' tacit knowledge*, [in:] *The Zlín University collection of Tomas Bata papers*, Zlín 2010, p. 132.

[21] L. Mládková, *Znalostní pracovníci v globalizovaném světě. Sborník Znalosti pro tržní praxi*, Olomouc 2010, pp. 277–282.

[22] R. Krishnaveni, R. Sujatha, *Communities of Practice: An Influencing Factor for Effective Knowledge Transfer in Organizations*, "IUP Journal of Knowledge Management", 2012, January, vol. 10, no. 1, pp. 26–40.

[23] G. Dean, P. Gottschalk, *Knowledge Management in Policing and Law Enforcement*, Oxford 2009, p. 17.

threat or when such threat is in a stage of its initial development. "An early warning system should be linked to control and information systems and should maintain a single line. At the same time, it should be linked to the knowledge management and the knowledge source".[24]

Tacit knowledge use in the Czech police – a survey

In November 2017, as part of the regular training of the top managers of the Police of the Czech Republic, a "round table" was held at which the results of the research in the field of knowledge management were presented, the existing situation was discussed and, finally, the participants were asked to fill in a questionnaire. The methods of transferring tacit knowledge (according to Krisnaveni and Sujatha as mentioned above) were presented, and the most commonly used methods, as well as those that should be used more, have been identified. The participants in the training and the respondents of the pilot questionnaire investigation were 12 top managers of the Police of the Czech Republic at the regional director level (or their deputies) and the directors of special nationwide units.

The questionnaire survey showed that the methods of transferring tacit knowledge that were mostly used according to top managers of the Police of the Czech Republic were the following: informal meetings, social networks and training. The methods of transferring tacit knowledge which, according to the respondents, should be used more were informal meetings, case studies, and active learning. The method of transferring tacit knowledge through informal meetings (as well as during official opportunities) was considered by the respondents as the crucial one.

The role of police management in boosting tacit knowledge exchange

Because of the character of tacit knowledge and its relation to its holders, the management of this type of knowledge cannot be separated from the human resource management, which is the essence of the work of each police managing officer, from the police president down to head of the lowest organizational unit of the police. It is important that line managers

[24] R. Zuzák, *Early Warning Systems for Strategic and Crisis Management, Knowledge for Market Use 2017*, [in:] *People in Economics – Decisions, Behavior and Normative Models, International Scientific Conference Proceedings*, Olomouc 2017, pp. 459–463, https://knowledgeconference.upol.cz/downloads/2017-Knowledge_for_Market_Use_Proceedings.pdf (accessed 10.08.2018).

lead and motivate their subordinates in sharing knowledge, intentionally help to create opportunities for personal meetings and intentionally build, over the long-term, an environment that supports mutual communication and trust, which is the basic precondition of policemen's willingness to share knowledge with one another. Practice confirmed the difficulty of knowledge transfer. Previous research[25] within the Police of the Czech Republic has demonstrated that knowledge is considered as a competitive advantage and sharing all the knowledge as a risk.

Conclusion

Fuzzy problems in security management and solving them require the optimal final assignment of the weight values of individual decision criteria in each dimensions and, at the same time, continuous updating. The extended concept of the internal and external security of the state, which distinguishes between four dimensions of security (ideals, values and the mental wealth of man; social influences, organizations and legal systems; the material aspects of human existence; the space and cybernetic space) was presented.

Criminal activity has become more sophisticated, its structure has changed, the seriousness of criminal activities against society is increasing. These facts, combined with the higher latency of crime, place increased demands on the activities connected with the search for criminals and on the overall work of the officers of the Police of the Czech Republic, their education and their knowledge.

The contribution draws attention to the methods of transfer of tacit knowledge and presents the most important methods, which are, according to the respondents (top managers of the Police of the Czech Republic), the most used: informal meetings, social networks and training, as well as the methods which should be used more intensively: informal meeting, case studies and active learning. Further research in this area may involve a greater number of respondents and more detailed mapping of the conditions of the transfer of knowledge at different levels of the organization.

[25] D. Junková, *Uplatnění znalostního managementu ve veřejném sektoru a v policejních sborech*, "Bezpečnostní teorie a praxe", 2013, no. 3, pp. 83–90.

References

1. Bradford B., Jauregui B., Loader I., Steinberg J., *Global Policing*, London 2016.
2. Dean G., Gottschalk P., *Knowledge Management in Policing and Law Enforcement,* Oxford 2009.
3. Hislop D., *Knowledge management in organizations: a critical introduction*, Oxford 2013.
4. Jirásek P., Novák L., Požár J., *Cyber security glossary*, Prague 2015.
5. Junková D., *Uplatnění znalostního managementu ve veřejném sektoru a v policejních sborech*, "Bezpečnostní teorie a praxe", 2013, no. 3, pp. 83–90.
6. Kný M., Junková D., *Vlivové faktory bezpečnostního managementu*, "Kultura Bezpieczeństwa. Nauka – Praktyka – Refleksje", 2017, no. 28, pp. 124–135, https://doi.org/10.24356/KB/28/5.
7. Kolářová K., *Kyberkriminalita v Česku vzrostla za sedm let téměř čtyřnásobně*, "Lidovky.cz", http://ceskapozice.lidovky.cz/kyberkriminalita-v-cesku-vzrostla-za-sedm-let-temer-ctyrnasobne-phi-/tema.aspx?c=A180515_171751_pozice-tema_lube (accessed 29.06.2018).
8. Kolouch J., *CyberCrime*, Prague 2016.
9. Kolouch J., *Kyberprostor*, Praha 2016, http://www.teorieib.cz/pbi/files/281-Kyberprostor-Kolouch.pdf (accessed 23.06.2018).
10. *Koncepce rozvoje Policie České republiky do roku 2020 (aktualizace 2017)* [Concept of the development of the Police of the Czech Republic up to 2020 (updated in 2017)], http://www.ceska-justice.cz/wp-content/uploads/2017/04/Koncepce-rozvoje-Policie.pdf (accessed 26.06.2018).
11. Krishnaveni R., Sujatha R., *Communities of Practice: An Influencing Factor for Effective Knowledge Transfer in Organizations*, "IUP Journal of Knowledge Management", 2012, January, vol. 10, no. 1, pp. 26–40.
12. Mládková L., *Znalostní pracovníci v globalizovaném světě. Sborník Znalosti pro tržní praxi*, Olomouc 2010, pp. 277–282.
13. Piwowarski J., *Three Pillars of Security Culture*, "Security Dimensions. International and National Studies", 2015, no. 14, pp. 10–16, https://doi.org/10.5604/01.3001.0012.5891.
14. Rice J.L, Rice B.S., *The Applicability of the SECI model to Multi--organisational endeavours: an integrative review*, "International Journal of Organisational Behaviour", 2009, vol. 9, no. 8, pp. 671–682.
15. Švec V., *What Do We Know About Tacit Knowledge? Development of managers' tacit knowledge*, [in:] *The Zlín University collection of Tomas Bata papers*, Zlín 2010, pp. 130–135.

16. *The "Deep Web" is Not All Dark*, https://i2.wp.com/www.deepwebtech.com/wp-content/uploads/DeepvsDarkIceberg.jpg (accessed 29.06.2018).
17. Veber J. *et al.*, *Management. Základy – moderní manažerské přístupy – výkonnost a prosperita*, Praha 2009.
18. Vysoký P., *Fuzzy logics – fashion or a paradigm change?*, "Vesmír", 1994, no. 6, p. 73, https://vesmir.cz/cz/casopis/archiv-casopisu/1994/cislo-6/fuzzy-logika-moda-ci-zmena-paradigmatu.html (accessed 05.04.2018).
19. Zuzák R., *Early Warning Systems for Strategic and Crisis Management, Knowledge for Market Use 2017*, [in:] *People in Economics – Decisions, Behavior and Normative Models, International Scientific Conference Proceedings,* Olomouc 2017, pp. 459–463, https://knowledgeconference.upol.cz/downloads/2017-Knowledge_for_Market_Use_Proceedings.pdf (accessed 10.08.2018).

CITE THIS ARTICLE AS:
D. Junková, M. Kný, *Fuzzy problems in security management: new threats and the importance of tacit knowledge in the Police of the Czech Republic*, [in:] *Security in Central and Eastern Europe: Cyberspace, Police, Prisons, Transport, Addictions, the Media. Proceedings from the Conference XLIV CICA: "Security in Europe" – 12th Security Forum Krakow, 5–7 June 2018, Kraków, Poland*, Krakow 2020, pp. 52–64, https://doi.org/10.24356/proceedings2018/2.

**SECURITY IN CENTRAL AND EASTERN EUROPE:
CYBERSPACE, POLICE, PRISONS, TRANSPORT, ADDICTIONS, THE MEDIA**
Proceedings from the Conference
XLIV CICA: "Security in Europe" – 12th Security Forum Krakow
5–7 June 2018, Kraków, Poland
2020 (65–89); https://doi.org/10.24356/proceedings2018/3

Cyber Attacks on Critical Information Infrastructure: Definitions, Threats and the Czech Perspective

Josef Požár*

ABSTRACT

Background: The contribution describes the situation concerning cyber security in the Czech Republic. Then it discusses the nature of cyber attacks and provides the definitions of cyber threats, cyber attacks as well as cyber attackers. The definition of critical information infrastructure is also part of the definition of critical infrastructure. **Objectives:** The purpose of the paper is to map the "terminological" situation in the Czech Republic, taking into account the chosen terms. **Methods:** Content analysis approaches are used, with an emphasis on the legal environment and, in part, the daily press discourse. **Results:** Some specific concepts from a transnational environment are being introduced gradually within the Czech Republic,

* Assoc. Prof. RNDr. Josef Požár, CSc., dr. h. c., Faculty of Biomedical Engineering of The Czech Technical University in Prague (CTU), Prague, Czech Republic; correspondence address: nám. Sítná 3105, 272 01 Kladno, Czech Republic; email: josef.pozar@fbmi.cvut.cz

however not always in a standardized way; the broader public does not know some terms or interprets them inconsistently. **Practical implications:** The practical effects of the contribution concern both teaching activities within the Police of the Academy of the Czech Republic in Prague and the permanent accreditation of terminological documents for the needs of public administration in the Czech Republic.

ARTICLE INFO

Article history
Received: 21.01.2019 Accepted: 4.04.2019

Keywords
cyber security, cybercrime, critical structure, critical information infrastructure, cyber attack, cyber threat

1. Introduction

The increasing cyber vulnerability[1] of modern society is the subject of long-term discussions at the European Union level as well as in the Czech Republic. The issue of the vulnerability of modern information systems and the means of protecting them against cybernetic attacks is a fundamental problem today. The functioning of the state as well as that of both state and private institutions is based on information systems representing the so-called critical infrastructure, including its part – critical information infrastructure. In this respect, vital questions need to be asked about the threats posed by cyber attacks not only to infrastructure but also to the population itself, and about the ways of counteracting these threats, such as efforts aimed at protecting the basic functions of the state, preventive measures, as well as efforts to maintain preparedness and to manage the possible consequences of extraordinary incidents.

Activities within the framework of the so called *critical infrastructure protection* belong among relatively new security priorities of the European Union, as well as the North Atlantic Treaty Organisation or their individual Member States, including the Czech Republic.[2]

[1] P. Jirásek, L. Novák, J. Požár, *Cyber security glossary*, Prague 2015, https://www.cybersecurity.cz/data/slovnik_v310.pdf (accessed: 11.01.2020), p. 137.

[2] It does not mean that some overlapping activities have not been performed previously, albeit under different names, for example activities related to *objects important for national defense* etc.

The basic principle of dealing with critical infrastructure is to ensure the functioning of key strategic infrastructures and to ensure protection of the population.

In January 2009, the document titled *Council Directive 2008/114/EC of 8 December 2008, on the Identification and Designation of European Critical Infrastructures and the Assessment of the Need to Improve Their Protection* came into force.[3] The document, among other things, defines the term *European Critical Infrastructure* (ECI) as critical infrastructure elements, located in the area of European Union Member States, whose disruption or destruction would mean a serious impact on at least two Member States. From all the originally indicated sections (Energetics; Nuclear Industry; Information and Communication Infrastructure; Water Industry; Food Industry; Health Care; Financial Sector; Transport; Chemical Industry; Space Research Facilities; Research Facilities) two have been mapped so far as ECI during the "test period": energy (electricity, oil, natural gas) and transport (road, rail, air, inland waterways, coastal and overseas shipping and ports).[4]

Selection of relevant operators of European Critical Infrastructure shall be governed mainly by cross-cutting criteria and other aspects, particularly as described in Annex III to the Directive. The test period expired on 12 January 2012. Since this moment a legislative review of that document is expected. The cross-cutting criteria are as follows:

- casualties criterion (assessed in terms of the potential number of fatalities or injuries), which might occur in case a specific infrastructure element is destroyed);
- economic effects criterion (assessed in terms of the significance of economic loss and/or degradation of products or services; including potential environmental effects);

[3] L. Harazin, O. Krulík, *The Czech Republic and Its Experience with Implementation of the Council Directive 2008/114/EC*, [in:] *Zbornik radova iz 5. međunarodnej konferencije "Dani kriznog upravljanja"; "Crisis Management Days"*, Velika Gorica 2012, pp. 801–814; *Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection (Text with EEA relevance)*, "Official Journal of the European Union", L 345, 23 December 2008.

[4] With regard to the existing European Union regulation and the challenges associated with these areas, the Czech Republic tends towards the future expansion of ECI, at least with regard to information and communication systems (ICT).

- public effects criterion (assessed in terms of the impact on public confidence, physical suffering and disruption of daily life; including the loss of essential services).

Every Member State, on whose territory some potential ECI element is located, was involved in bilateral or multilateral negotiations with other Member States for which that element (its destruction or non-functioning) may cause a serious impact. An exclusive right, however, to decide whether a particular element will or will not be considered the ECI element, belongs only to the state on whose territory this element is located. The Member States were obliged to identify the individual ECI elements, to equip these with appropriate documentation (crisis plans) and to appoint the so-called liaison security officers to work at these sites. Within the framework of the Czech Republic, this requirement has been accomplished.

Government of the Czech Republic, ministries and other central administrative authorities in the areas related to the critical infrastructure are key participants in the process of critical infrastructure protection. Individual owners or operators are going to be legally entrusted with the key responsibility for implementing measures to protect individual critical infrastructure elements. Main co-ordinator of this agenda is the General Directorate of the Fire Rescue Brigade of the Czech Republic.

At the beginning of 2011 an amendment of *Act No. 240/2000 Coll., on crisis management*, came into force which – among other things – complies at least formally with the requirements imposed in this context upon the Czech Republic by the European Union. With this step, the issue of critical infrastructure and its protection has become an integral part of the Czech Republic's crisis management strategy.[5]

The "industries" (areas) as well as the sectoral and cross-cutting criteria to be used in defining the critical infrastructure elements in the Czech Republic are best illustrated in the *Government Decree No. 432/2010 as of 22 December, 2010, on the criteria to be employed in the specification of critical infrastructure elements*.[6] The industries are defined as follows:

- Energetics – electricity, gas, heat energy, oil and petroleum products;

[5] L. Lukáš, M. Hromada, *Management of Protection of Czech Republic Critical Infrastructure Elements*, 2011, http://www.wseas.us/e-library/conferences/2011/lanzarote/acmos/acmos-59.pdf (accessed: 11.11.2019).

[6] L. Nečesal, L. Lukáš, *Entities of Critical Infrastructure Protection in the Czech Republic*, 2011, http://www.wseas.us/e-library/conferences/2011/lanzarote/acmos/acmos-76.pdf (accessed: 12.11.2019).

- Water management – supplies of drinking and utility water; securing and management of surface and underground water reserves; wastewater system;
- Food industry and agriculture – food production, food treatment, agricultural manufacture;
- Health care – pre-hospital emergency care; hospital care; public health protection; manufacture, storage and distribution of pharmaceuticals and medical devices;
- Transport – road, rail, air, inland water ways;
- Communication and information systems – services provided by fixed telecommunication networks, mobile telecommunication networks, radio communication and navigation, satellite communication, television and radio broadcast, internet access and access to data services, postal and courier services;
- Banking and finance sector – public finance management, banking, insurance, capital market;
- Emergency services – Fire Rescue Service of the Czech Republic, Police of the Czech Republic, Army of the Czech Republic, radiation monitoring including recommendations of protective measures, public alert and address systems;
- Public administration – social protection and employment, diplomacy, judiciary and prison service, public administration and local government.

However, further elaboration of the topic into "sub-sectors" may cause some embarrassment. Different areas (depending on the designated coordinators) are conceived into different detail (often too general or too detailed) or with differing comprehensibility. This area is apparently short of a unifying approach and most likely also the "common sense". Some sub-sectors have been designed in such a manner that it is difficult to imagine whether a single element falls into their category. By contrast, other sub-sectors are characterized by a flood of many different subjects that might fall under their category.

What is particularly problematic in this area is that, in most cases, **critical information infrastructure itself involves computer networks and transferring data through the Internet which is open and publicly accessible and has no geographic borders**. Therefore, securing and protection thereof requires not only the initiative of the state but also the assistance of inhabitants. The individual countries, including the Czech Republic, continuously build and increase national capacities in this area. However,

without the cooperation of the private sector and the academic sphere, and without intensive international cooperation and the involvement of the users of the Internet, the required efficiency of these activities cannot be ensured.

The Czech Republic certainly does not belong among the countries that would be understood as pathfinders for a CERT/CSIRT team in Europe. This only illustrates the little emphasis connected to information security issues in the Czech Republic in the past.

Although the Czech Republic has been connected to the Internet since 1993 or 1994, for a long time it was impossible to talk about a comprehensive security policy in this area.

The topic of establishing a team (hierarchy of teams) of the CERT/CSIRT type in the Czech Republic was one of the „chronic" aspects of the efforts related to the information security agenda in the Czech Republic for more than 10 years.

Very important is the fact that responsibility for information infrastructure in the Czech Republic has long been the subject of competence struggle (mostly a "negative" one, when no institution was willing to take the responsibility for the respective agenda).

Between the years 2003 and 2007, the Czech Republic had the Ministry of Informatics of the Czech Republic that was more or less responsible for the cybersecurity agenda. After the dissolution of this Ministry, the agenda was not completely transformed to another institutions, and it caused a period of disputes that had impact on the situation in the respective area for many years.

In 2006 and 2007, the process of building the National CERT/CSIRT team continued through the Consortium, which won the tender of the Security Research Project of the Ministry of the Interior of the Czech Republic for the period 2007–2010 (project called *Cyber Threats in the Security Interests of the Czech Republic*).[7]

The consortium also included the "academic" CESNET-CERTS team, the first domestic CERT/CSIRT team with relevant practical experience, already connected to the relevant transnational platforms. The process of building a **coordinating model workplace – team of CERT/CSIRT type** (CSIRT.CZ) within academic network CESNET started in mid 2007. Its

[7] The consortium was formed by individual faculties of the Charles University Prague, Czech Technical University, CESNET (Internet Service Provider for numerous academic institutions), and NESS Czech Company.

pilot operation was launched on 3 April 2008. The team has been continuously organizing methodical education (with the participation of a number of private entities, representatives of the Security Information Service, the Police of the Czech Republic and the National Security Authority). During its existence, CSIRT.CZ has gained a reputation at home and abroad, but its formal international accreditation was blocked due to the uncertainty about its future after the end of the project.

For foreign counterparts situation in the Czech Republic became even more unclear. Two competing "CERT/CSIRT" teams were confusing for them.

In **September 2008**, the security team of NIC.CZ[8] (CZ.NIC-CSIRT) was created. The effectiveness of this team has been so far the most advanced of all teams of this type in the Czech Republic. A number of incidents was vigorously resolved, not only "archived" through this team.

Despite all partial shifts, **political consensus** on practical steps towards building a national CERT/CSIRT-type team **had not been achieved since 2007 until the beginning of 2010**. At a later stage, the responsibilities (and costs) associated with this step were refused by the Ministry of the Interior of the Czech Republic, the Ministry of Defense of the Czech Republic as well as the National Security Authority of the Czech Republic. It is no wonder that these delays caused embarrassment not only in the domestic expert community.

The situation (at least for some time) started to clarify after introduction of the caretaker government in the Czech Republic (June 2009 to July 2010), especially due the Resolution of the National Security Council of **5 January 2010** No. 4, titled *On the Analysis of the Current Level of Cyber Security of the Czech Republic*. This document imposed the main competences and responsibility for the next steps regarding the cybersecurity agenda unambiguously on the Ministry of the Interior of the Czech Republic.

[8] CZ.NIC is an association of legal persons founded in 1998 by the leading Internet service providers in the Czech Republic. The main activity of the association is the operation of the domain name register.cz. At present, the association is improving the domain management system, supporting new technologies beneficial to the Internet infrastructure in the Czech Republic. CZ.NIC is a member of international organizations that associate similar organizations around the world (CENTR, ccNSO and others) and also a member of EURid, a European.eu domain.

Following the aforementioned Resolution of the National Security Council, a new Cyber Security Department was established within the Ministry of the Interior of the Czech Republic at the beginning of 2010.

One of its first registrable activities was the participation at the session of the CSIRT.CZ Working Group on **25 March 2010** (interconnecting representatives of major internet service providers, content providers, state security forces, Czech Telecommunication Office, CZ.NIC, NIX.CZ[9] and the academic sector).

But no tangible steps were then taken by the state (the Ministry of the Interior of the Czech Republic), and the initiative was taken over by the private sector, especially by the administrator of the Czech national domain, CZ.NIC. At its own expenses and responsibility, it created a CERT/CSIRT-type team that used the company background and served to the widest public. This situation continued until 16 December 2010, when a Memorandum on Computer Security Incident Response Team of the Czech Republic was signed between the Ministry of the Interior of the Czech Republic and the CZ.NIC, according to which the CZ.NIC temporarily (from 1 January 2011) took the agenda of the national security team CSIRT.CZ.

The Memorandum also stated that the Ministry of the Interior of the Czech Republic addressed the status of CERT/CSIRT teams within the state administration and sought to support the inclusion of CSIRT.CZ in international structures, in particular by confirming the status of CSIRT.CZ as a national CSIRT team. Furthermore, it coordinates the activities of CSIRT.CZ, evaluates information received from CSIRT.CZ in case CSIRT.CZ suspects that the incident could have an impact on the state or state administration systems. The Ministry of the Interior of the Czech Republic also had the right to request an audit of the performance of CSIRT.CZ activities.

As it was already stated above, CSIRT.CZ was a research project carried by CESNET that ended on 31 December 2010. As of **1 January 2011**,

[9] NIX.CZ (Neutral Internet Exchange) is a platform that interconnects Internet Service Providers in the Czech Republic by connecting together their Internet networks. Telecommunication companies operating in the Czech Republic form this association because they have a common interest in ensuring that their computer networks are mutually interconnected and their customers can quickly communicate via the Internet within the country. Members of the platform contribute together to the technologies that can improve the exchange efficiency and security.

under the agreement of the Cyber Security Department of the Ministry of the Interior of the Czech Republic, the CESNET and CZ.NIC, took the responsibility for the relevant equipment to be able to maintain the continuity of CSIRT.CZ.

CSIRT.CZ, perceived as a national CSIRT team since its creation, became in 2010 a co-worker of the European Union Agency for Information Technology (Point of Contact for the Czech Republic).

In connection with the aforementioned facts, the National Security Council of the Czech Republic discussed on **28 February 2011** the document describing the then situation regarding the cyber security issues in the Czech Republic. Due to the importance of the agenda, the Cyber Security Strategy (elaborated by the Ministry of the Interior of the Czech Republic) was submitted to the National Security Council and then to Government by **30 June 2011**.

The perspectives regarding the various stages of possible development, as expected in the beginning of 2011, were described by the following visualizations (several CERT/CSIRT-type teams, two of them open to the general public questions and proposals).

1.1 Transfer of the agenda to the National Security Authority of the Czech Republic

The "coordinative role" of the Ministry of the Interior of the Czech Republic did not last long. On the basis of Resolution of the Government of **19 October 2011** No. 781, titled *On the Umbrella National Authority Responsible for the Area of Information Security Regarding the Public Sector of the Czech Republic*, the relevant competence was transferred to the National Security Authority of the Czech Republic. The new administrator was already, whether alone or in co-operation with other stakeholders, very active in many relevant areas. The Government approved the establishment of the National Cyber Security Center as a part of the National Security Authority of the Czech Republic.

At the same time, the Government of the Czech Republic set up the Cyber Security Council as a part of the National Security Council and the National Cyber Security Center as a part of the National Security Authority of the Czech Republic. At the same time, the Government imposed a number of specific tasks on the National Security Authority of the Czech Republic. Relevant Cyber Security Strategy for the years **2012 to 2015** was

already elaborated also under the coordination of the National Security Authority of the Czech Republic.

In January 2012, CSIRT.CZ reviewed the period of one year of its operation with the following conclusion: The CSIRT.CZ team officially represented the Czech Republic in the world (in the relevant international forums and as the first contact point for foreign counterparts). In July 2011 it organized the pilot training seminar *The World of the Internet and Domains*, intended for employees of the state administration and members of the security forces, especially the Police of the Czech Republic. The team was cooperating with Internet Service Providers in the Czech Republic. Special attention was paid to the practical issues that should help (especially) the police investigators to orient themselves in the issue of basic forms of cybercrime and to learn to address directly the specific subjects that can support their work. Participants of the pilot course were also the intelligence operations specialists, judges etc. In 2011, CSIRT.CZ was invited to Law Enforcement Authorities Expert Working Group of European Union Agency for Information Technology. The work of this expert group resulted in a document mapping the experience raised from the interconnection of law enforcement and cybersecurity experts, and suggesting a set of recommendations.

This cooperation did not end in 2012. Because of the fact that the National Security Authority of the Czech Republic was not able to launch its Gov-CERT, that was already "underway" in the former premises of the Ministry of Defense in Brno), the decision was made to sign another Memorandum, moving this "turning point" until 2015. Until then, the national cyberspace was to be dominated by the CZ.NIC.

1.2 Proposal of the modified institutional framework

A proposal was given in which one of the first drafts of the *Act on Cyber Security* (February 2012) included framework for the provision of information security functions in the Czech Republic. It was envisaged to create two umbrella CERT/CSIRT teams in the Czech Republic:

1) The **"national" CERT** was to be built on the fundament of the CZ.NIC (CSIRT.CZ), with the use of experience of the model workplace-team operated by CESNET (CSIRT.CZ) according to the research project of the Ministry of Interior of the Czech Republic. The "national" CERT will establish or deepen existing links with and among similar teams within the Network Monitoring Cluster and, in the first phase, perhaps,

also regarding the public sector. CSIRT.CZ will be involved in resolving cyber-security incidents in networks operated in the Czech Republic. CSIRT.CZ will also provide co-ordination assistance, but not physical support, to resolve individual incidents (but this assistance will not be provided directly to end users). CSIRT.CZ will collect and evaluate data on reported incidents and report respective incidents to those responsible for operating the individual network(s) that is (are) the source(s) of the incident, in accordance with the severity of the incident. CSIRT.CZ will fulfill the role of so-called National Point of Contact (PoC), as well as the center of education and dissemination of cyber security-related education. It will also assist to establish the CERT/CSIRT teams in networks operated in the Czech Republic, including the help regarding the establishing of co-operation connections with foreign/global security platforms.

2) At the same time (or later) the construction of the **"government" CERT** team (GovCERT.CZ) would be launched. This team would be primarily designed to monitor government networks and (public) critical information infrastructure, or to coordinate and methodologically run other sub-centers of this type that operate or will operate within specific public institutions.[10]

In connection with the construction of this team, it seems especially necessary[11] to interconnect both platforms, as well as ensure their connection to the "military" team of a similar type (CIRC.CZ).

Both teams are to be understood first and foremost as partners who "lighten each other's burdens". However, GovCERT would have a veto right in a number of questions, but at the same time it does not possess such technical and human resources (it is reportedly a problem to fill the relevant positions in public institutions), such as the National CERT that was built mainly on the basis of CZ.NIC.

[10] The National Cyber Security Center will pursue efforts to protect networks primarily within public institutions, such as ministries, energy companies, hospitals, or the Czech National Bank. The National Center for Cyber Security (in its embryonic condition) is directly subordinate to the Director of the Office.

[11] Due to the fact that there are several platforms in the Czech Republic already bearing the name CERT or CSIRT, it was decided that this "governmental" concept would differentiate (as in other countries) by the prefix "Gov" (derived from the word *government* or *governmental*). In addition, this term indicates the "superiority" of such a platform over the other CERTs (CSIRTs) existing within the state.

The whole process is planned to go from "more limited" to "more ambitious" goals. The relevant experts saw this proposal as a shift in the positive direction (compared with many years of inactivity in the past).[12] The limits related to the involved bodies (important and unimportant public administration information systems as well as "selected" service providers and network operators) were not entirely clear.

1.3 Gradual stabilization: towards National Cyber and Information Security Agency (2012–2017)

On **19 December 2014** the regulations implementing the *Law No. 181/2014 on Cyber Security* were published in the Collection of Laws:

- *Regulation No. 316/2014 Coll. on Security Measures, Cyber Security Incidents and Reactive Measures*;
- *Regulation No. 317/2014 Coll. on the Determination of Important Information Systems and their Determination Criteria*;
- *Decision of the Government No 315/2014 Coll. which amends the Decision of the Government No. 432/2010 Coll. on the Criteria for the Determination of the Elements of the Critical Infrastructure*.

The Act No. 181/2014 Coll. on the Cyber Security and on the Amendments of the Related Acts (Cyber Security Law) after many discussions and changes, became effective on **1 January 2015**. The Act on Cyber Security is „based" on two principles: The first principle is to minimize the interference with the rights of private persons; the second is the principle of individual responsibility for the security of respective information systems. The Act came into force together with implementing regulations.

In **August 2017** National Cyber and Information Security Agency (NCISA) became the central body of state administration for cyber security, including the protection of classified information in the area of information and communication systems and cryptographic protection. It is also in charge of the public regulated service of the Galileo satellite system. It was created on the basis of Act No. 205/2017 Coll., amending Act No. 181/2014 Coll., on the Cyber Security and on the Amendments of the Related Acts (Cyber Security Act).

[12] At the same time it is said that this concept could be improved and reshaped along with the development in countries that are more developed in the field of information security (for example, Germany).

National Cyber and Information Security Agency with its 120 employees took over the agenda of the National Security Authority of the Czech Republic that previously fell under the responsibility of the National Cyber Security Center that had been operating since 2011. National Cyber and Information Security Agency's headquarter in Brno is located in offices that previously served National Cyber Security Center.

The situation in the Czech Republic grew closer to what is considered standard in advanced European countries.

Main areas of the activity of **National Cyber and Information Security Agency** are as follows:

- operating of the Government CERT (GovCERT.CZ);
- cooperation with other domestic CERT/CSIRT teams;
- cooperation with international CERT/CSIRT teams;
- drafting of security standards for information system regarding critical information infrastructure and "important information systems" (defined by law);
- support of education in the field of cyber security;
- research and development in the area of cyber security;
- protection of classified information in the field of information and communication systems and cryptographic protection.

National Cyber and Information Security Agency operates National Public Regulated Service Center (NCPRS), which fulfils the task of the so-called Competent Public Regulated Service Authority; it is one of the services provided by the European satellite system Galileo.

A new building in barrack premises in Brno is planned to be built that will serve almost 400 staff members. The new office should be opened in 2023.[13]

In this area, it is not possible to only rely on a simple description of security with the help of the so-called "CIA" triad, which stands for Confidentiality, Integrity and Availability. Cybernetic security is not only a set of valueless technical solutions – if it was, it would legitimize the absolute removal of the distribution rights for security purposes. When it comes to the necessity of ensuring security (this being a non-contributory right), the

[13] O. Krulík, *Milestones, Related to the Development of Organizational Aspects of the Cybersecurity and Protection against Cyber-Threats in the Czech Republic*, "Academic and Applied Research in Military and Public Management Science", 2018, vol. 17, no. 3, pp. 115–130, https://search.proquest.com/openview/8c8a16f387533f34132b8c2c7e5f581e/1?pq-origsite=gscholar&cbl=4378877 (accessed: 11.11.2019).

individual freedoms of individuals must be restricted (i.e. their distributive[14] rights, including the right for privacy). However, this solidarity restriction must be proportionate. The level of the admissibility of restricting personal freedoms for the sake of security is extensively discussed across jurisdictions. The components of the principle of proportionality between security and individual rights were stated by the Constitutional Court of the Czech Republic in File No. 4/1994 of 12 October 1994[15], which sets the following criteria: suitability, necessity and the comparison of the gravity of the conflicting rights. In this relation, the respective concept also mentions the so-called "optimising order" as the maximum use of possible means for the purpose of minimising the restriction of rights which in a particular case must retreat as part of the proportionality test. So, the proportionality test is not only used to exclude extreme disproportion, but also to balance the affected rights in particular situations. The proportionality test must be an integral part of any legislative effort in the security area. An excessive prevalence of the executive breaches the distributive rights of users, including the right for privacy.

The objective of the paper is to provide the reader with knowledge about the relation of the critical information infrastructure and cybernetic security.

2. Cybernetic security and critical infrastructure – terminology

The terminology that is to be described here mainly comes from such areas as the critical infrastructures of the state, as well as various areas of cybernetics. **Critical infrastructure** is the elements or groups of elements (structures, facilities, means of public infrastructure) and their operators, the breaching of whose function may have a serious effect on the security of the state. Critical infrastructure provides for the basic life needs of inhabitants, the health of people and the economy of the state. Security as a system category requires a system approach so that protection could be provided for individuals, enterprises and state institutions against attacks aimed at their destruction and other cybernetic attacks that could threaten the func-

[14] *Distributive and commutative justice*, [in:] *Rights and justice in international relations*, "OpenLearn", n.d., https://www.open.edu/openlearn/people-politics-law/politics-policy-people/politics/rights-and-justice-international-relations/content-section-4.1 (accessed: 11.11.2019).

[15] *Usnesení ústavního soudu České republiky*, 12.10.1994, https://nalus.usoud.cz/Search/GetText.aspx?sz=Pl-4-94 (accessed: 11.01.2019).

tioning of state institutions and bodies. This system approach is, among others, manifested in sectoral criteria, i.e. technical or operating values for determining the elements of the critical infrastructure and the energy sector, water management, food industry and agriculture, health system, transport, communication and information systems, financial market and currency, emergency services and public administration.

The definition of *critical infrastructure* provided by Jirásek, Novák and Požár is as follows: "systems and services which would have a serious impact on state security, its economy, public administration and the basic needs of inhabitants if they are not functioning or function badly".[16] The same source defines *critical information infrastructure*: "complete information and communication systems (meeting the stated criteria and sectoral criteria for cyber security), which could have a serious impact on state security, including the capability of ensuring the basic life needs of inhabitants, the health of people and the state economy if not functioning".[17] The term *cyber space* is defined as "the digital environment for creating, processing and exchanging information consisting of information systems, services and electronic communications networks".[18] Another definition *of cyber space* characterises it as a "set of mutually linked computer technology networks, including services, computer systems, single purpose systems, with built-in bus-bars and information stored on storage media during the running through networks".[19]

The best-known cyber space is without doubt the Internet – a global computer network. Other examples of cyber spaces may include Intranets, metropolitan networks, etc. Any set of interconnected computer networks used for communication meets the definition of cyber space (internets with lowercase 'i'). The Oxford Dictionary defines the term cyber space as an "imaginary environment in which communication takes place through computer networks".[20] In the context of organizations, cyber space is one or more mutually linked local computer networks (e.g. LAN, i.e. Local Area

[16] *Council Directive 2008/114/EC of 8 December 2008…*, *op. cit.*; P. Jirásek, L. Novák, J. Požár, *Cyber security…*, *op. cit.*, p. 66.

[17] *Ibidem*, p. 65.

[18] *Ibidem*, p. 70.

[19] J. Kruliš, *How to win risks: active risk management – management tool of successful firms*, Prague 2011, p. 25.

[20] *Cyberspace*, "Lexico", 2016, http://www.oxforddictionaries.com/us/definition/american_english/cyberspace (accessed: 21.03.2016).

Network). A network that interconnects local networks is called a WAN (Wide Area Network). Examples of cyber spaces that are not connected to the Internet network are military computer networks, technological networks, police data networks, etc.

Risks originating from the existence of cyber space may have a far-reaching impact. The mutual dependence of systems and cyber spaces must be considered a vulnerability. A *cyber system* is a system that uses cyber space.[21] According to Bertalanffy, a system can be defined as "complete elements in mutual interaction". In other words, "[a] system is elements that are bound to each other by a relationship or relation and as a whole this system has a relation to its surroundings".[22] The system is not only set of elements, but those whole mutual relations create the whole unit.

Such a system includes an information infrastructure, employees and other entities dealing with the business processes and the behaviour of the system. By nature, cybernetic systems today are part of most organizations. They are always present. Inhabitants, organizations and whole governments rely today on computer systems and the Internet. Some critical infrastructure services (i.e. the elements or systems that as mentioned above, if interfered with, would have a serious impact on state security, the basic life needs of inhabitants, health of people and the state economy; critical infrastructure in the Czech Republic is specified in Section 2 letter g) of *Act No. 240/2000 Coll., Crisis Act*, and *Government Directive No. 432/2010 Coll., on the criteria for determining elements of critical infrastructure*),[23] are provided owing to cyber systems.

Cybernetic security, or *cyber security*, is a set of means of protecting cybernetic systems against cybernetic threats. A *cybernetic threat* is a threat that exists because of the existence of cyber space. Here, threat means any reason or unwanted incident that may result in damage to the system or organisation.[24]

Cyber security mainly refers to removing threats against which assets must be protected. Cyber security mainly protects information or infrastructure assets.

[21] J. Kruliš, *How…*, *op. cit.*, p. 26.

[22] J. Habr, J. Vepřek, *Systémová analýza a syntéza*, Praha 1986, p. 26.

[23] *Zákon č. 430/2010 Sb. Zákon, kterým se mění zákon č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů (krizový zákon), ve znění pozdějších předpisů*, 30.12.2010.

[24] P. Jirásek, L. Novák, J. Požár, *Cyber security…*, *op. cit.*, p. 52.

Therefore, it is necessary to distinguish between information security and cybernetic security. *Information security* mainly ensures the confidentiality, integrity and availability of information. Information can be recorded in various forms: electronically, physically, or even by means of the knowledge of the personnel. For information security to be maintained, information in all forms must be protected against threats and the originators of threats, including physical, human-made and technological threats.

Cybernetic security is protection against threats that occur in cyber space. These threats may endanger information assets and, therefore, information security is an important part of cybernetic security. Cybernetic security only deals with information assets that can be accessed in cyber space.

Cyber security is not only restricted to protecting information assets. It also deals with protecting infrastructure and in the wider context (when a given information system does not directly affect the real world), also with the indirect protection of assets existing in the real world (for example, protecting life, health, reputation, etc.).

Many sources on cyber security interconnect cybernetic security and information security. For the correct understanding of the principles of cybernetic security, these terms must be separated. Similarly, information security is not restricted by its content to threats from cyber space.

3. Contemporary cyber threats

As the issue of cyber security not only concerns the private sector but also the public sector, these issues are highly valid at the national and international level. Specialised institutions are being created with the objective of identifying, with the help of highly qualified experts, the weaknesses of the cybernetic systems. This is done by creating standardized methods and procedures of cyber risk management, by protecting critical data and state systems, and last but not least, by fighting, in an efficient way, against cyber incidents and attackers.

At present there is a rapid increase in the number of highly organised cyber space attacks, whose purposes are, for example, to steal information and/or financial means, or to breach or destroy critical infrastructure or information systems. Similarly, the perpetrators of traditional criminal activities such as child pornography, banking and financial frauds, intellectual property theft, industrial espionage and many others, find today in cyber space a great field for operation. The issues of terrorism and organised

crime cannot be omitted; they mainly manifest themselves in cyber space through ingeniously designed websites.

At present it is very difficult to protect cyber space against these activities for various reasons. Attackers do not need physical contact with the technology due to global interconnection, they can operate from any part of the world and because of routing through many servers, they can remain anonymous. This does not only involve attacks on vulnerable individuals, or slightly better protected companies; it also involves massive attacks against critical infrastructure that may have principal effects on the defence systems or the economies of whole countries. Therefore, the issue of cyber security has become one of the main priorities of individual states in recent years.

The reports of respected companies, such as PwC, Deloitte or Symantec, were analysed to gather objective data.[25] For example, the antivirus provider, Symantec, ascertained in 2018 more than 460 million new malwares[26] (year-on-year increase 36 %) and 329 successful attacks during which more than 429 million pieces of personal data were stolen.[27] Each day up to one million user accounts are attacked. In addition, it was reported that Symantec alone were blocking more than 1 million attacks a day on their web sites (2018).[28]

Smart phones are often attacked irrespective of the operating system. In 2015, about 1.4 billion smartphones were sold and the estimate for 2020 assumes a significant increase. Unlike desktop computers and notebooks, smart phones and tablets are much less protected or are not protected at all. The same situation applies to the Internet of Things.[29]

4. Czech Republic and cyber threats to critical infrastructure

Because of the high level of mutual interconnections between individual industries, critical infrastructure is endangered in a complex way by natural, technological and asymmetric threats. Mainly, the functioning of the

[25] An audit and antivirus company.

[26] Harmful software, i.e. a program designed to penetrate or damage a computer system.

[27] Symantec, *Internet Security Threat Report*, April 2016, vol. 21, https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-appendices-en.pdf (accessed: 2.04.2017).

[28] Symantec, *Internet Security Threat Report*, February 2018, vol. 24, https://www.symantec.com/content/dam/symantec/docs/reports/istr-24-2019-en.pdf (accessed: 2.01.2020).

[29] *The Internet of things: First International Conference, IOT 2008: Zurich, Switzerland, March 26–28, 2008: proceedings*, C. Floerkemeier, M. Langheinrich, E. Fleisch, F. Mattern, S.E. Sarma (eds), Berlin 2008.

energy infrastructure is threatened by political pressures, as well as criminal threats. These threats include e.g. politically motivated manipulations of strategic raw material supplies, or the use of other potentially risky capital. These potential adverse actions are targeted at the critical infrastructure of the Czech Republic via e.g. sabotage, cyber attacks and economic crime.

With regard to the threat of cyber attacks, the priorities of the Czech government include securing the critical information infrastructure and important information systems through a Government coordination office[30] whose task is to respond immediately to cyber security incidents. The authorities of Czech Republic support the building of the systems that will enable general cooperation of all players involved in cyber security, i.e. also those that are not part of the public administration and yet may contribute to the exchange of experiences in solving cyber incidents at the national and international level. The government enforces legislative and non-legislative measures so as to be in accord with the principles of the development of the information society and the Czech National cyber security strategy for 2015–2020.[31]

5. Cyberattacks and their forms

At present, the most frequent cyberattacks are those on hardware, software, processed or stored data and networks. One of the methods of classifying cyber attacks is specifying the target, i.e. whether they aim at an individual (user), at individual applications or at the infrastructure. Another classification of cyberattacks is presented by Jirovský[32]:

- leaks of information when the subject's protected information is disclosed without authorisation;
- a breach of data integrity, i.e. the damage, alteration or complete destruction of data;

[30] *Rada vlády pro informační společnost*, "Vláda České republiky", 16.06.2010, https://www.vlada.cz/cz/media-centrum/predstavujeme/rada-vlady-pro-informacni-spolecnost-73632/ (accessed: 3.08.2020).

[31] *Národní strategie kybernetické bezpečnosti České republiky na období let 2015 až 2020*, "ENISA – European Union Agency for Cybersecurity", 30 March 2015, https://www.enisa.europa.eu/about-enisa/structure-organization/national-liaison-office/news-from-the-member-states/czech-republic-national-cyber-security-strategy-2015-2020 (accessed: 2.01.2019).

[32] V. Jirovský, *Cyber crime: not only about hacking, cracking, viruses and Trojan horses without secret*, Prague 2007.

- service suppression that intentionally prevents access to information, applications or systems (for example, overloading e-shop pages so that normal users cannot access them);[33]
- non-legitimate use, i.e. use by an unauthorized subject or in an unauthorized way.

During a successful cyber-attack, one of three basic[34] elements of cyber security is disrupted i.e. people's activities, technology or processes.

While this issue may seem irrelevant, the use of unauthorized software may open up significant potential for further attacks. Users breach copyright while using software for personal needs as well as in commercial use with the aim to achieve a profit. The motivation may be unwillingness to invest in legal software (illegal software is used or licences are used by more users then permitted). A common example of such activity is downloading copyright-protected music, films and other products. A very similar risk is hidden in so-called freeware, i.e. programmes offered free of charge (or with the acceptance of hidden adverts in it).

At present there are many tools for disrupting cyber security.[35]

- **Hacking**. A traditional hacking attack can be divided into five phases: survey, scanning, gathering access, maintaining access and smoothing tracks. The first phase, survey, is in fact the most important. During this phase, the hacker does not do anything against the target system and only collects information, i.e. data about the use of IP addresses, DNS records, post server, etc.
- **Phishing**. This is a method of fraud,[36] which tries to steal the digital identity of a user, i.e. his/her passwords, bank card number, internet banking access, with the aim of consequently stealing financial means. This is mostly done by creating a false message usually sent by e-mail by which the hacker tries to gather the necessary data. It can be a fabricated query from a financial institution to verify the password or account number or a request from an e-shop to verify a credit card number or PIN. The message is masked as trustworthy and it imitates with maximum precision the communication of the financial institution. When the user becomes

[33] For example DoS – Denial of Service.

[34] Systems, data and information must be protected against disruption of confidentiality, availability and integrity during their whole service life.

[35] P. Voříšek, *Threats and attacks from cyber space*, [in:] *Security theory and practice*, Prague 2014, pp. 3–20.

[36] P. Jirásek, L. Novák, J. Požár, *Cyber security…*, *op. cit.*, p. 82.

assured that he/she is really communicating with a financial institution and fills in and sends the required data, his/her accounts and payment cards are misused.[37] These attacks are mainly targeted at individual users. This type of attack is largely facilitated by the naïve approach of many users. Moreover, phishing tools are offered on the market from 2–10 dollars and their usage does not require special technical capabilities. A more dangerous and more sophisticated form of phishing is **pharming**. This is a fraudulent method38 used on the Internet to gather sensitive data from the attacked victim. Phishing and pharming are forms of attack on one's personal details. A criminal will use them to obtain one's user names and passwords. However, while their premise is the same – their method is different. Phishing attacks will usually involve an email that appears to be from a company with which one does business. Tricking a user into thinking this email has come from a legitimate source, a phishing email will prompt him/her to log in to any account with the link provided in the email. The website the user visits is not real, but has been created to mimic the layout and design of the legitimate page. However, as it appears authentic, a user enters his/her username and password, which is then captured by the attacker.

Pharming is different. A pharming attack can happen even when one is browsing a legitimate site and one has typed in the URL of the website one's own. In a pharming attack, the criminal "hijacks" the intended site's DNS (domain name system) server and the result is that a user is redirected to an imposter site. Much like in a phishing scam, many won't notice any difference, and will enter their username and password as usual, and the attacker captures it.

- **Sniffing**.[39] Another method of attack that the end user practically does not register is sniffing. This is a method of illegally capturing data passing through information networks.
- **Ransomware**. This is a cyber racket where the programme encrypts data and demands the user to pay in order to gain access it. In most cases it is a so-called Trojan horse or virus.

[37] L. James, *Phishing without mysteries*, Prague 2007.

[38] P. Jirásek, L. Novák, J. Požár, *Cyber security…*, *op. cit.*

[39] *Ibidem*, p. 106.

- **Denial of Service (DoS)**[40] is an attack conducted through web pages and their server with the aim of overloading the service with high numbers of display requests. This therefore prevents access for other normal users. Another way of attacking is **Distributed Denial of Service (DDoS)**, where a large number of distributed computers (so-called zombies) are routed to targets at the same time, which results in overloading the targets' services.
- **Data Encryption.** This is an old way of storing and transferring data so that they can only be read by the sender of the message and the addressee. So, it is a process by which unsecured electronic data is converted using cryptography to encrypt data which can only be read by the owners of the decryption key. Encryption is used to protect the data against undesired ascertainment by another person and is used when storing and transferring data, including telecommunication.

In practice, with the development of new information technologies, there is a series of new virus attacks on critical information infrastructures. In August 2019, the number of new computer viruses increased more than twice compared with the previous month. During last month, throughout the world, 3,300 new viruses were spread, as well as worms, Trojan horses and other harmful software items. One month ago, the anti-virus company, TrendMicro, registered 1,400 new viruses. Virus attacks on computer networks, since their shy beginnings, have also become more sophisticated. The objective of their creators and users is to earn large sums of money by gathering so-called sensitive data. The main interests of cyber attackers are passwords, personal data and access to bank applications.

6. Conclusion

The increase in the frequency and sophistication of cyberattacks is mainly caused by the massive development of information and communication technologies that are used by individuals, organisations and the state. As new information and communication technologies interfere with numerous spheres of the functioning of both the private and public sector, an efficiently functioning system must be created that can react very flexibly to the changing conditions.

[40] In 2013 in the Czech Republic attacks were registered, for example, on Novinky.cz, Seznam.cz, iHned.cz, E15.cz.

Along with the existing trends the capabilities of the cyber world are used on a still wider scale; what in the past was only available to the citizens of developed countries with large budgets is now also within the reach of other countries. At the same time, these opportunities open the risk of attacks on cybernetic systems. This is because the existing modern economic, political and military systems depend more than at any other time in the past on information and instructions generated in cyber space and transferred by huge systems.

The importance of information and communication technologies will continue to grow, as well as the importance of attacks against them.

Cyber threats will continue to develop and their creators will keep on searching for vulnerable places in new software, applications and facilities. Information and communication technologies users can be protected by maintaining appropriate security measures during on-line activities, utilising up-to-date security software and updating all security applications with the latest security patches.

There is great interest in cyber security as regards hardware, literature, foreign contacts, competent personnel and, in case of policemen, as regards training special police unit dealing with discovering and investigating cyber crime. As far as the competent cyber security-related personnel is concerned, it is necessary to mainly focus on outstanding younger experts, fresh graduates from universities and talented IT fans with a good command of foreign language.

References

1. *Act No. 240/2000 Coll., Crisis Act* [Zákon č. 240/2000 Sb. Zákon o krizovém řízení a o změně některých zákonů (krizový zákon)], "Poslanecká sněmovna Parlamentu České republiky", 2000, https://www.psp.cz/sqw/sbirka.sqw?cz=240&r=2000 (accessed: 15.10.2016).
2. *Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection (Text with EEA relevance)*, "Official Journal of the European Union", L 345, 23 December 2008.
3. *Cyberspace*, "Lexico", 2016, http://www.oxforddictionaries.com/us/definition/american_english/cyberspace (accessed: 21.03.2016).
4. *Distributive and commutative justice*, [in:] *Rights and justice in international relations*, "OpenLearn", n.d., https://www.open.edu/openlearn/people-

politics-law/politics-policy-people/politics/rights-and-justice-international-relations/content-section-4.1 (accessed: 11.11.2019).
5. Habr J., Vepřek J., *Systémová analýza a syntéza*. Praha 1986.
6. Harazin L., Krulík O., *The Czech Republic and Its Experience with Implementation of the Council Directive 2008/114/EC*, [in:] *Zbornik radova iz 5. međunarodnej konferencije "Dani kriznog upravljanja"; "Crisis Management Days"*, Velika Gorica 2012, pp. 801–814.
7. *The Internet of things: First International Conference, IOT 2008: Zurich, Switzerland, March 26–28, 2008: proceedings*, C. Floerkemeier, M. Langheinrich,E. Fleisch, F. Mattern, S.E. Sarma (eds), Berlin 2008.
8. James L., *Phishing without mysteries*, Prague 2007.
9. Jirásek P., Novák L., Požár J., *Cyber security glossary*, Prague 2015, https://www.cybersecurity.cz/data/slovnik_v310.pdf (accessed: 11.01.2020).
10. Jirovský V., *Cyber crime: not only about hacking, cracking, viruses and Trojan horses without secret*, Prague 2007.
11. Krulík, O., *Milestones, Related to the Development of Organizational Aspects of the Cybersecurity and Protection against Cyber-Threats in the Czech Republic*, "Academic and Applied Research in Military and Public Management Science", 2018, vol. 17, no. 3, pp. 115–130, https://search.proquest.com/openview/8c8a16f387533f34132b8c2c7e5f581e/1?pq-origsite=gscholar&cbl=4378877 (accessed: 11.11.2019).
12. Kruliš J., *How to win risks: active risk management – management tool of successful firms*, Prague 2011.
13. Lukáš L., Hromada M., *Management of Protection of Czech Republic Critical Infrastructure Elements*, 2011, http://www.wseas.us/e-library/conferences/2011/lanzarote/acmos/acmos-59.pdf (accessed: 11.11.2019).
14. *Národní strategie kybernetické bezpečnosti České republiky na období let 2015 až 2020*, "ENISA – European Union Agency for Cybersecurity", 30 March 2015, https://www.enisa.europa.eu/about-enisa/structure-organization/national-liaison-office/news-from-the-member-states/czech-republic-national-cyber-security-strategy-2015-2020 (accessed: 2.01.2020).
15. Nečesal L., Lukáš L., *Entities of Critical Infrastructure Protection in the Czech Republic*, 2011, http://www.wseas.us/e-library/conferences/2011/lanzarote/acmos/acmos-76.pdf (accessed: 12.11.2019).
16. *Rada vlády pro informační společnost*, "Vláda České republiky", 16.06.2010, https://www.vlada.cz/cz/media-centrum/predstavujeme/rada-vlady-pro-informacni-spolecnost-73632/ (accessed: 3.08.2020).

17. Symantec, *Internet Security Threat Report*, April 2016, vol. 21, https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-appendices-en.pdf (accessed: 2.04.2017).
18. Symantec, *Internet Security Threat Report*, February 2018, vol. 24, https://www.symantec.com/content/dam/symantec/docs/reports/istr-24-2019-en.pdf (accessed: 2.01.2020).
19. *Usnesení ústavního soudu České republiky*, 12.10.1994, https://nalus.usoud.cz/Search/GetText.aspx?sz=Pl-4-94 (accessed: 11.01.2020).
20. Voříšek P., *Threats and attacks from cyber space*, [in:] *Security theory and practice,* Prague 2014, pp. 3–20.
21. *Zákon č. 430/2010 Sb. Zákon, kterým se mění zákon č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů (krizový zákon), ve znění pozdějších předpisů*. 30.12.2010.

CITE THIS ARTICLE AS:
J. Požár, *Cyber attacks on critical information infrastructure: definitions, threats and the Czech perspective*, [in:] *Security in Central and Eastern Europe: Cyberspace, Police, Prisons, Transport, Addictions, the Media. Proceedings from the Conference XLIV CICA: "Security in Europe" – 12th Security Forum Krakow, 5–7 June 2018, Kraków, Poland*, Krakow 2020, pp. 65–89, https://doi.org/10.24356/proceedings2018/3.

**SECURITY IN CENTRAL AND EASTERN EUROPE:
CYBERSPACE, POLICE, PRISONS, TRANSPORT, ADDICTIONS, THE MEDIA**
Proceedings from the Conference
XLIV CICA: "Security in Europe" – 12th Security Forum Krakow
5–7 June 2018, Kraków, Poland
2020 (90–104); https://doi.org/10.24356/proceedings2018/4

Radicalisation – Definition, Models, Detection in Czech Prisons

Štěpán Strnad*
Štefan Danics**

ABSTRACT

The aim of the article is to present the methods of identifying radicalised persons through their psychological and social characteristics and the application of these methods of detecting prisoners' radical predispositions and tendencies within the Czech prison system. An example of a tool for identifying the process of radicalisation in prisons is the Czech police's pilot project SAIRO, whose objective is the timely detection of warning signals which accompany the radicalisation of an individual and a classification of the prison population. The methodological basis of the pilot project is the detection of outer noticeable signals in the process of a person's transformation, so called indicators of radicalisation, which represent

* Štěpán Strnad, Mgr. Ph.D., Police Academy of the Czech Republic in Prague, Prague, Czech Republic; correspondence address: Lhotecká 559/7, 143 01 Prague 4, Czech Republic; email: strnad@polac.cz
** Štefan Danics, Doc. Ing. Ph.D., Police Academy Czech Republic in Prague, Prague, Czech Republic.

visual, behavioural, rhetoric and other aspects of the person's behavioural metamorphosis. The authors describe the characteristic features of the radicalisation process and specify the definition of radicalisation. The authors also emphasize that, as current research shows, radicalisation can proceed very differently in each individual, i.e. there does not exist a universal model of radicalisation.

ARTICLE INFO

Article history
Received: 14.06.2018 Accepted: 4.04.2019

Keywords
radicalisation, indicators, detection, prisons, models of radicalisation

Introduction[1]

In Europe, the topic of radicalisation appeared in academic discussions after the bomb attacks in Madrid (2004) and London (2005), while, in the process of conceptualisation, the term *violent radicalisation* has been created after 2001 relating to the terrorist attacks on the symbols of US power. Regarding this, it is important to notice that the terms *radicalisation* or *violent radicalisation*, *extremism*, and *terrorism* are not synonymous with one another. Radicalisation is a broad term, while extremism and terrorism are narrower terms which stand at some distance from the mainstream political thinking and are mainly linked with violence against civilians.

Radicalisation has become one of the keywords of our time; it is one of the main focuses of the media as well as scientific, political and social discourses. Today, there are different conceptions of radicalisation as well as diverse research approaches and models. Experts also diverge concerning the identification of the causes and developmental stages of radicalisation. It is not surprising that there is often confusion or an overlap of the above concepts causing frequent misunderstandings and problems for further research. They are multidisciplinary terms as they are examined from different viewpoints, i.e. by different experts from different areas of social sciences, which results in significantly non-uniform terminology and perception

[1] The article was created within a scientific task 2/3 *Symbolism of criminal tattoos at PACR in Prague, Czech Republic*.

regarding radicalisation. Currently, the radicalisation problem is reduced only to the terrorist threat, which considerably narrows the scope of the concept and the prevention possibilities against terrorist attacks. We can effectively counteract radical and extremist views and ideologies rather than terrorism itself, because terrorism represent the oldest method of conflict resolution, and that is why the elimination of ideologies that lead to active that method, is seen as the most needed.

The authors purport to draw attention to the current issues concerning the conceptualisation of radicalisation and to juxtapose these research problems with the reality of the Czech prison environment. Radicalisation is perceived by the authors as a multi-layered and internally contradictory social process that is framed by various identifying factors. The authors highlight the identifiers of radicalisation in the prison environment, as well as the concepts that are currently being applied to the Czech prison environment for the purpose of researching this phenomenon.

The concept of radicalisation

Since the 1970s, the term radicalisation has been applied both to describe the interactions between social movements and the state and to refer to the gradual escalation of social violence. In this understanding of radicalisation, the users of the term referred to their own use of violence in different forms and intensities, i.e. the dynamics of social violence was examined. Radicalisation could be, according to the then users of the term, understood as **a process leading to the increased use of political violence, being the result of the transformation of values, the political polarization of certain social groups, and the articulation, as well as enforcement, of the radical interests of the society.**

Radicalisation process may also escalate into the open hostility towards certain social groups or social institutions and structures in a given society.

Ashour and Boucek talk about radicalisation as a transformation process of certain social groups going through an ideological or behavioural change which, according to them, leads to the rejection of democratic principles including the rejection of legitimate political pluralism.[2]

[2] O. Ashour, C. Boucek, *De-Radicalisation in Egypt, Algeria, and Libya*, "Carnegie Endowment for International Peace", 16.04.2009, http://carnegieendowment.org/2009/04/16/de-radicalization-in-egypt-algeria-and-libya/201v (accessed 2.05.2014).

In the analyses of radicalisation, various approaches thereto are being distinguished, such as *top-down radicalisation* and *bottom-up radicalisation*. Experts characterise *top-down radicalisation* as an ideological way of thinking about violent acts. In turn, *bottom-up radicalisation* takes place when individuals or groups are thinking about becoming violent and are seeking the ideological grounds for their potential violence. Based on this, it is possible to distinguish the range and nature of actors involved in radicalisation.

Although the very existence of the process of radicalisation is generally accepted in scientific circles, difficulties arise when it is necessary to define *radicals* and *extremists*, although it is generally agreed that *extremists* hold ideas and goals which are contradictory to the values of a given society and intend to carry out their political goals regardless of the freedom and life of other citizens. Radicalisation is mostly described as the process which is trying to cause dissatisfaction among individuals and groups with the current social and political system, with the aim to change the system. However, not all radicals intend to use violence to change the system. The question is when non-violent strategies become inefficient and depleted and at which point violence starts to be considered as a legitimate means of a radical change.

The process of radicalisation can be understood as an increasing presence of anti-liberal and anti-democratic elements and values in social thinking and behaviour, whether at the level of individuals or entire social groups. In the process of radicalisation, individuals (alone or being a part of a social group) become exposed to extremist ideas which they gradually absorb and, as a consequence, their attitudes change.[3]

Although there has not been any uniform or universally accepted technical definition of *radicalisation*, there is a general consensus that "radicalisation is currently a commonly used term to describe what is going on before the bomb goes off", and it is to be understood as "a sequence of processes influenced by different factors".[4] Radicalisation is also conceptualised as "the process of beliefs acquisition, including a willingness to use violence

[3] Š. Danics, L. Tejchmanová, *Extremismus, radikalismus, populismus a euroskepticismus*, 1st edition, Praha 2017, p. 91.

[4] *Prisons and Terrorism. Radicalisation and De-radicalisation in 15 Countries*, "International Centre for the Study of Radicalisation", 2010, http://icsr.info/wp-content/uploads/2012/10/1277699166PrisonsandTerrorismRadicalisationandDeradicalisationin15Countries.pdf (accessed 20.09.2016).

as a method of effective social change".[5] It should be emphasised that the conclusion on radicalism being "what is going on before the bomb goes off" is authored by Peter Neumann, an expert from the International Centre for the Study of Radicalisation (ICSR). This thesis clarifies that people are not born as extremists and terrorists, but they are becoming ones in the process of radicalisation.

The models of radicalisation

The concept of radicalisation is today heavily debated as there is a dispute whether it can be defined as a repeatable "process" or as a completely context-specific, individual set of factors that cannot be precisely documented. The dispute is about whether a certain set of characteristics and indicators renders a certain individual more likely to use violence than the others. Most studies suggest that there is no single motive nor path that would lead one to engage in violent radicalism. Radicalisation is understood by experts as a process of change to which some people are more prone provided that certain causal events and factors are present.

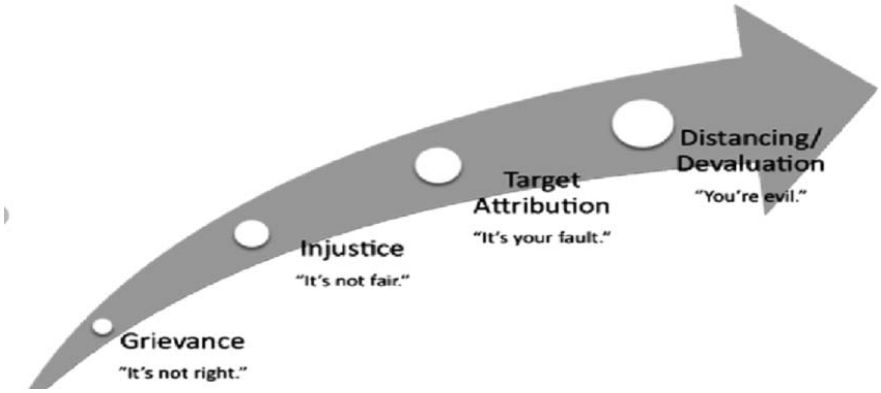
The authors focus on **five major models of radicalisation** which are today discussed and cited in the academic as well as the political world:

- **Borum's four-step model** (2003) – in this model, the description of the process starts at the moment when extremist thoughts start to mature in an individual and these trigger radicalisation, which results in terrorism. At the first stage, the individual, facing a specific event, realizes the unfairness of a certain condition. At the second stage, this condition is being compared against other groups in the society to assure the individual about injustice. At the third stage, a culprit is searched for and the last stage follows when culprits are identified as the evil ones which must be eliminated (thus violence becomes justified).[6]

[5] C.E. Allen, *Written testimony of Charles E. Allen, Assistant Secretary for Intelligence and Analysis, Chief Intelligence Officer, Department of Homeland Security "Threat of Islamic Radicalization to the Homeland"*, "The Investigative Project on Terrorism", 14.03.2007, p. 4, https://www.investigativeproject.org/documents/testimony/270.pdf (accessed 20.07.2017).

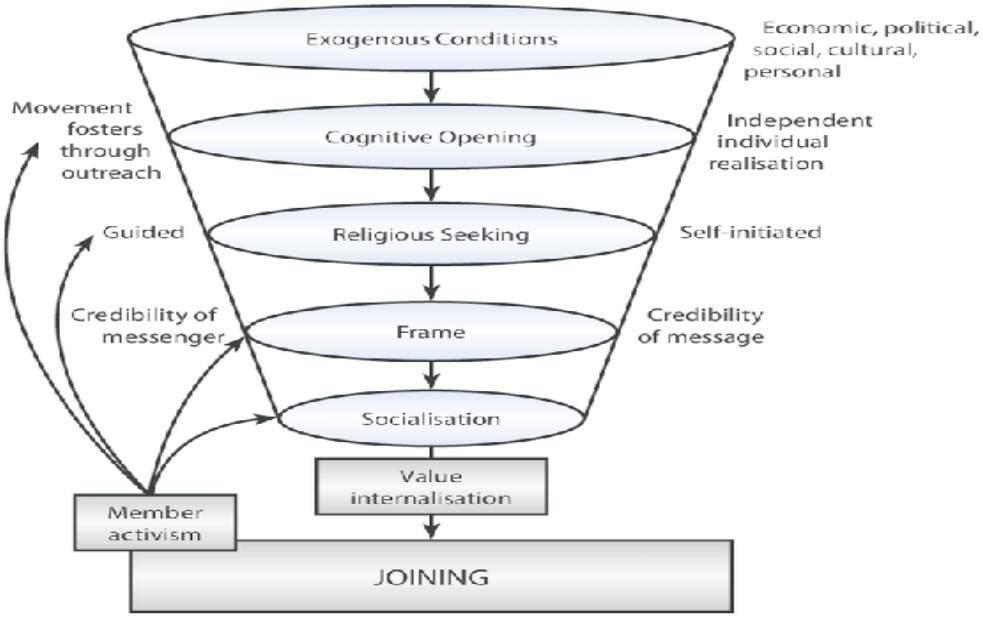
[6] R. Borum, *Radicalization into Violent Extremism II: A Review of Conceptual Models and Empirical Research*, "Journal of Strategic Security", 2011, vol. 4, no. 4, pp. 37–62, https://doi.org/10.5038/1944-0472.4.4.2.

Fig. 1. Four-stages Borum's model



Source: R. Borum., *Radicalization into Violent Extremism I: A Review of Social Science Theories*, "Journal of Strategic Security", 2011, vol. 4, no. 4, p. 39, https://doi.org/10.5038/1944-0472.4.4.1.

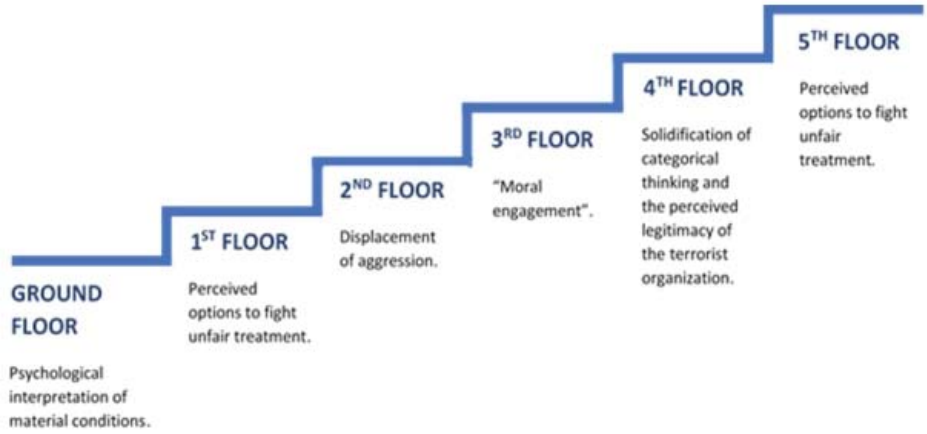
Fig. 2. Wiktorowicz's model



Source: A.J. Beutel, *Building Bridges to Strengthen America. Forging an Effective Counterterrorism Enterprise Between Muslim Americans and Law Enforcement*, Washington D.C. – Los Angeles 2009, p. 9.

- **Wiktorowicz's model** (2005) – it emphasises the social context and the influence of the closest people on the radicalisation of individuals. There are four key processes that increase the probability of an individual being attracted by a radical group with subsequent active involvement. The model is depicted graphically as a gradually narrowing funnel on top of which the external factors are located. These can include economic, socio-cultural, personality-related and/or political factors which lead to experiencing discrimination and to an increased proneness to extremist thoughts. At this stage, self-radicalisation occurs either on the basis of one's own impulses or under the command of already radicalised people.[7]

Fig. 3. Moghaddam's staircase model



Source: L.J. Lorenzo-Penalva, *Situational Understanding on Violent Radicalization that Results in Terrorism. Two Graphic Models that Provide Clarity on the Topic*, "Grupo de Estudios en Seguridad Internacional (GESI), University of Granada", 2018, http://www.seguridadinternacional.es/?q=en/content/group (accessed 20.09.2016).

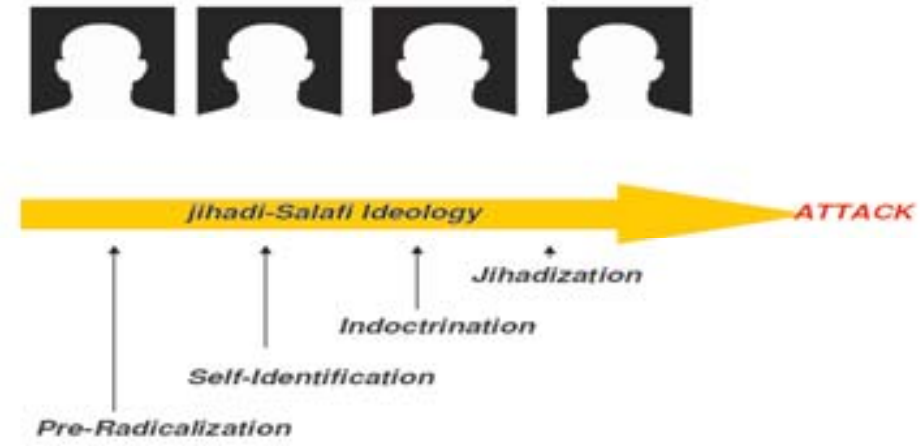
- **Moghaddam's six-step model** (2005/6) – a staircase scheme in which radicalisation is viewed as a process, i.e. advancing up the stairs where every next step reduces the probability of an individual moving back and avoiding radicalisation.[8]

[7] Q. Wiktorowicz, *Joining the cause: Al-Muhajiroun and radical Islam*, "Syracuse University Institute for National Security and Counterterrorism", 2004, http://insct.syr.edu/wp-content/uploads/2013/03/Wiktorowicz.Joining-the-Cause.pdf (accessed 22.02.2018).

[8] F. Moghaddam, *The Staircase to Terrorism: A Psychological Exploration*, "American Psychologist", 2005, no. 60(2), pp. 161–169, http://fathalimoghaddam.com/wp-content/

- **New York four-step model** (2007) – designed by the members of the New York Police Department and security services together with scientists and leading anti-terrorist experts: they analysed Madrid (2004) and London (2005) terrorist attacks and have provided a detailed look at terrorists and the reasons for their radicalisation.[9]

Fig. 4. New York Police Model



Source: M.D. Silber, A. Bhatt, *Radicalization in the West: The Homegrown Threat*, "The New York City Police Department", 2007, p. 19, https://sethgodin.typepad.com/seths_blog/files/NYPD_Report-Radicalization_in_the_West.pdf (accessed 10.07.2017).

- **Sageman's four-step model** (2004-2008) – it stresses the importance of social ties in the process of radicalisation.[10]

All models but Sageman's are linear models in which the target individual gradually moves down the path towards violent extremism. In Sageman's model, the four corners are not linear, as they may affect individuals either

uploads/2013/10/1256627851.pdf, https://doi.org/10.1037/0003-066X.60.2.161 (accessed 22.02.2018).

[9] M.D. Silber, A. Bhatt, *Radicalization in the West: The Homegrown Threat*, "The New York City Police Department", 2007, https://sethgodin.typepad.com/seths_blog/files/NYPD_Report-Radicalization_in_the_West.pdf (accessed 22.02.2018).

[10] M. Sageman, *Radicalization of Global Islamist Terrorists*, "United States Senate Committee on Homeland Security and Governmental Affairs", 27.06.2007, https://www.hsgac.senate.gov/download/062707sageman (accessed 22.02.2018).

all at a time or in different combinations. In these models, there is a number of interesting factors. All but one describe radicalisation as a process with identifiable stages or elements, and they do it linearly. The consequences of this fact for policymakers are clear: these models could be used institutionally for the training of analysts and security personnel to follow the signs of radicalisation.

Radicalisation in prisons

In the European context, the issue of radicalisation and de-radicalisation has been resonating in the professional, public and political discourse for several years. The primary security issue is now the timely identification of radicalised individuals and the ability of security forces to detect the persons that pose a threat to security by engaging in violent extremist and terrorist groups. Radicalisation in prisons is not a new phenomenon. The prison environment worldwide is historically a recruiting ground for extremist groups of different ideological and religious orientations. The risk of radicalisation in such environment is enhanced by the accumulation of such factors as the nature of the prison community in which one meets individuals with a criminal record, often also with propensity for relapse, who are likely to display socio-pathological behaviour and a higher degree of psychological predisposition to radicalisation.

Although the radicalisation of people in prisons is an international phenomenon, the specific national form is mainly influenced by cultural specificity, the organization of the national prison system and facilities, the prison subculture, the presence of racist attitudes and nationalism in this community, the degree of cohesion and mutual loyalty of prisoners, social norms, traditions, or local and regional customs.[11] There are a number of typologies of prison populations. According to Jones, one can divide convicts into two groups according to the character of their criminal activities. The first group is represented by the so-called mainstream prisoners, i.e. the perpetrators of traditional general crimes (property, drug, or violent crimes). The second group is composed of persons sentenced for the support or the promotion of extremist attitudes, or for the pursuance of extremist violence. The unlawful conduct of the latter group is based on ideological motives. The risk of the latter group getting in touch with the first one lies

[11] B. Vegrichtová, *Radikalizační procesy v prostředí věznic a možnosti jejich identifikace*, "Státní zastupitelství", 2018, no. 1, pp. 42–53.

in the so-called ideological infection and the expansion of the circle of the sympathizers and members of extremist groups.[12]

One can notice certain signals of the radicalisation process in prisoners' behaviour. These signals are called the indicators of radicalisation, which can be traced in changes in the appearance of the person concerned, their actions or verbal expressions. These do not necessarily mean that the person is willing to commit an offence of violence. These are seen as warning signs of the radicalisation process. However, it is not possible to establish a universally valid identification methodology of the radicalisation process, or a universally valid set of identifiers that are met by those committing acts of extreme violence or terrorist attacks. A number of indicators applied to the environment of prisons is identical to the indicators of the radicalisation of any other social environment. The main objective of the recognition of the identifiers of radicalisation is the timely detection of radicalised individuals who are under the risk of being recruited, indoctrinated or encouraged to criminal activities with ideological motives.

Identifiers of radicalisation and the SAIRO programme

Since 2013, the Section for Terrorism and Extremism of National Centre against Organized Crime (STE NCOZ) of the Czech Republic has been cooperating with the General Directorate Prison Service of the Czech Republic (GŘ VS) in the field of detecting the radicalisation of persons in custody and during their sentence. Based on the cooperation, the pilot **SAIRO (Systém analytické identifikace radikalizovaných osob – System of Analytical Identification of Radicalised Individuals) programme** has been set up, whose purpose is the identification of the signs of radicalisation in prisons. The detection of radicalisation has so far been conducted by a number of bodies; however, their activities have not been centrally coordinated, there has been no exchange of information, and some activities may have been duplicated without a coherent and uniform framework of practical application.

Experience from abroad confirms the necessity of close information exchange between the involved state branches which need to undertake interdepartmental cooperation. The project, whose objective is the estab-

[12] R.C. Jones, *Are prisons really schools for terrorism? Challenging the rhetoric on prison radicalization*, "Punishment and Society", 2014, vol. 16, no. 1, pp. 74–103, https://doi.org/10.1177/1462474513506482.

lishment of Coordination Centre for the Detection of Radicalisation in Prisons and the subsequent de-radicalisation of the affected persons, has a preventive character. The aim is not the stigmatisation of the detected persons, but the protection of an affected individual and society as a whole against the radicalisation process. The working group of the coordination centre should consist of the members of security forces, judicial bodies and scientific-research institutions. It could include the members of the Police (PCR), the Supreme Public Prosecutor's Office (NSZ), the Police Academy (PA CR), the National Centre against Organized Crime (NCOZ), the Prison Service (VS CR), the Probation and Mediation Service (PAM) and the Security Intelligence Service (BIS), as well as the Military Police and experts from various bodies dealing with radicalisation.

The SAIRO programme comprises the following stages: the observation of the behaviours of the accused and the convicted, the follow-up evaluation, the implementation of a dedicated type of analysis and the implementation of a suitable re-socialisation programme, which has not yet been, unfortunately, implemented in practice in today's Czech prison system as a means of de-radicalisation. The programme is based on the collection of data and information through the observation of the behaviour of the accused and the convicted, carried out by the Prison Service staff. Individual displays of prisoners are evaluated using a set of indicators to which certain point values are assigned by the computer program. By combining individual indicators of radicalisation, a mathematical algorithm then establishes the percentage of risk of the radicalisation of a given individual. Further, the information on the selected persons is revised, the authenticity of the individual's behaviour is examined and measures to de-radicalise the person are taken.

Along with the establishment of the Coordination Centre for the Detection of Radicalisation in Prisons, a working group is being formed for the detection of radicalisation, as well as a working group for de-radicalisation. The existing practice points out the necessity to create the third group, dedicated to the coordination of education. The question remains whether this group should be subordinate to the first two mentioned groups and work within them, or whether it should work independently and be based on the same requirements as the first two groups. The intention of the project is to create a centre which is an umbrella working group for the interdepartmental cooperation in the field of anti-extremist policy. The project is therefore made up of two parts, the first – DETECTION and the second – DE-RADICALISATION. The first part is based on the

programme SAIRO (System of Analytical Identification of Radicalised Individuals), on further training courses for the Prison Service staff and on the academic research. The second part of the project is in the process of preparation.

Each of the components of the project is going to include a defined range of activities. The activities of the working group for the detection of radicalisation are carried out by individual institutions according to their specialisation. The activities of the working group for de-radicalisation are now at the stage of conceptualization. These activities should include collecting data and information from the SAIRO programme based on the risks assessment of radicalized persons. Furthermore, the working group should include specialists that will work with the radicalised persons and propose recommendations for their treatment. Each radicalised person requires an individual approach and depending on the case, separation, integration or isolation may be suggested. The first option is a preventive measure aimed at limiting the further spread of radicalisation and ideological contagion, as well as at separating the persons from the charismatic leader of the group. The second option is suitable for the rehabilitation process of the less involved individuals in an extremist group; it reduces the risks of radicalisation not only in the person concerned but also in the whole prison community. The third option is designed for the most dangerous persons, leaders and recruiters.

Among other procedures and tools to be used by the de-radicalisation working group, thorough psychological profiling should be included, as well as the analysis of the radicalisation process of a given individual on the basis of the exchange of information between the involved security forces, courts, religious organizations, medical facilities, etc. The success rate of detection and de-radicalisation depends on the degree of training of the staff in charge of collecting primary data and information and recording them to the SAIRO programme. The Prison Service staff is also vulnerable to the threat of radicalisation and cooperation with radicalised persons. Finally yet importantly, the emphasis must be put on the design and implementation of rehabilitation programmes that should become part of the integration process of former extremists.

Within the pilot project, certified training of Prison Service staff has already been conducted, in the field of radicalism, extremism and terrorism. It was a follow-up of the training within the SAIRO programme, conducted under the auspices of the Police Academy of the Czech Republic

in Prague. At the same time, different versions of the SAIRO programme, suitable for other institutions, are being prepared. The legislative aspects of this programme are also being elaborated. The original aim of the SAIRO programme, dedicated to Czech prisons, has been extended due to the interest of other security bodies in implementing the system of detection of radicalised individuals into their agenda. A central information system for the detection of radicalised individuals is currently being designed. It is based on the liaison of individual interested security bodies. One day, a version of the programme may be released that will be segmented and adjusted to the needs of individual interested bodies, so that each organ has its own secure environment for their work. Among potential advantages, there are prompt access to information, smooth link-up and simplicity in administering the programme.

Conclusion

One of the key methodological issues in detecting radicalised persons is the relation between the degree of the person's involvement and their willingness to commit a certain offence (even criminal). By the degree of involvement, the authors understand one's passive participation in public or non-public activism (demonstrations, protests, blockades, concerts, etc.) without active involvement in any organization or commitment to crimes. By the degree of willingness to commit a certain offence (even criminal), the authors mean active involvement in public or non-public radical activities including organizational or managerial involvement. The aim is to create the scale of a person's susceptibility to the risk of radicalisation, on the basis of a set of indicators, which would work with the three groups of people, i.e. 1) informative group, reporting low risk; 2) interest group, demonstrating signs of extremism but not following an organised group (passive supporters and sympathizers); and 3) risky/potentially dangerous group (persons detected in the interest group who proved willing to actively engage in violent extremist activities).

Not only radicalisation in prison environment but also radicalisation in the whole society requires the multidisciplinary approach and the comprehensive procedures of prevention, repression and rehabilitation. The basic role in the identification of high-risk individuals in prisons is played by the Prison Service; however, comprehensive and effective detection, as well as the mitigation of the radicalisation process in an individual, require the involvement of Probation and Mediation Service staff, psychologists,

educators, social workers and, last but not least, academics. The cooperation between the institutions and their experts is crucial for the timely identification of radicalisation, its evaluation, the assessment of its degree and the initiation of preventive measures, all of which play a vital role both for the sake of the de-radicalisation of an individual and for the overall protection of society.

References

1. Allen C. E., *Written testimony of Charles E. Allen, Assistant Secretary for Intelligence and Analysis, Chief Intelligence Officer, Department of Homeland Security "Threat of Islamic Radicalization to the Homeland"*, "The Investigative Project on Terrorism", 14.03.2007, https://www.investigativeproject.org/documents/testimony/270.pdf (accessed 20.07.2017).
2. Ashour O., Boucek C., *De-Radicalisation in Egypt, Algeria, and Libya*, "Carnegie Endowment for Inter-national Peace", 16.04.2009, http://carnegieendowment.org/2009/04/16/de-radicalization-in-egypt-algeria-and-libya/201v (accessed: 2.05.2014).
3. Beutel A.J., *Building Bridges to Strengthen America. Forging an Effective Counterterrorism Enterprise Between Muslim Americans and Law Enforcement*, Washington D.C. – Los Angeles 2009.
4. Borum R., *Radicalization into Violent Extremism I: A Review of Social Science Theories*, "Journal of Strategic Security", 2011, vol. 4, no. 4, pp. 7–36, https://doi.org/10.5038/1944-0472.4.4.1.
5. Borum R., *Radicalization into Violent Extremism II: A Review of Conceptual Models and Empirical Research*, "Journal of Strategic Security", 2011, vol. 4, no. 4, pp. 37–62, https://doi.org/10.5038/1944-0472.4.4.2.
6. Danics Š., Tejchmanová L., *Extremismus, radikalismus, populismus a euroskepticismus*, 1st edition, Praha 2017.
7. Jones R.C., *Are prisons really schools for terrorism? Challenging the rhetoric on prison radicalization*, "Punishment and Society", 2014, vol. 16, no. 1, pp. 74–103, https://doi.org/10.1177/1462474513506482.
8. Moghaddam F., *The Staircase to Terrorism: A Psychological Exploration*, "American Psychologist", 2005, no. 60(2), pp. 161–169, http://fathalimoghaddam.com/wp content/uploads/2013/10/1256627851.pdf, https://doi.org/10.1037/0003-066X.60.2.161 (accessed 22.02.2018).
9. Lorenzo-Penalva L.J., *Situational Understanding on Violent Radicalization that Results in Terrorism. Two Graphic Models that Provide Clarity on the Topic*, "Grupo de Estudios en Seguridad Internacional (GESI), University

of Granada", 2018, http://www.seguridadinternacional.es/?q=en/content/group (accessed 20.09.2016).
10. *Prisons and Terrorism. Radicalisation and De-radicalisation in 15 Countries*, "International Centre for the Study of Radicalisation", 2010, http://icsr.info/wp-content/uploads/2012/10/1277699166PrisonsandTerrorismRadicalisationandDeradicalisationin15Countries.pdf (accessed 20.09.2016).
11. Sageman M., *Radicalization of Global Islamist Terrorists*, "United States Senate Committee on Homeland Security and Governmental Affairs", 27.06.2007, https://www.hsgac.senate.gov/download/062707sageman (accessed 10.07.2017).
12. Silber M.D., Bhatt A., *Radicalization in the West: The Homegrown Threat*, "The New York City Police Department", 2007, https://sethgodin.typepad.com/seths_blog/files/NYPD_Report-Radicalization_in_the_West.pdf (accessed 10.07.2017).
13. Vegrichtová B., *Radikalizační procesy v prostředí věznic a možnosti jejich identifikace*, "Státní zastupitelství", 2018, no. 1, pp. 42–53.
14. Wiktorowicz Q., *Joining the cause: Al-Muhajiroun and radical Islam*, "Syracuse University Institute for National Security and Counter-terrorism", 2004, http://insct.syr.edu/wpcontent/uploads/2013/03/Wiktorowicz.Joining-the-Cause.pdf (accessed 10.07.2017).

CITE THIS ARTICLE AS:
Š. Strnad, Š. Danics, *Radicalisation – definition, models, detection in Czech prisons*, [in:] *Security in Central and Eastern Europe: Cyberspace, Police, Prisons, Transport, Addictions, the Media. Proceedings from the Conference XLIV CICA: "Security in Europe" – 12th Security Forum Krakow, 5–7 June 2018, Kraków, Poland*, Krakow 2020, pp. 90–104, https://doi.org/10.24356/proceedings2018/4.

TRANSPORT SECURITY IN UKRAINE

**SECURITY IN CENTRAL AND EASTERN EUROPE:
CYBERSPACE, POLICE, PRISONS, TRANSPORT, ADDICTIONS, THE MEDIA**
Proceedings from the Conference
XLIV CICA: "Security in Europe" – 12th Security Forum Krakow
5–7 June 2018, Kraków, Poland
2020 (106–118); https://doi.org/10.24356/proceedings2018/5

Safe Transportation of Goods in the Supply Chain of Contemporary Ukraine: Risk Management and Means of Loading Safety

Larysa Yankovska*
Ilona Petryk**

ABSTRACT

The article analyzes the safety of cargo transportation in Ukraine. The stages of transportation risk assessment and management are described, both of them being vital ways of ensuring the safe transportation of goods in modern conditions. The importance of ensuring the safe transportation of cargoes in Ukraine is determined and its practical application by enterprises in Ukraine is analyzed. The specialty of the transportation of dangerous and large-sized cargoes by enterprises of Ukraine is worked out. The evaluation of statistical information on the transportation of goods on the territory of

* Larysa Yankovska, Doctor of Economics, Lviv University of Business and Law, Lviv, Ukraine; correspondence address: Lviv University of Business and Law, Kulparkivska st., 99, Lviv 79000, Ukraine; email: business_law@ukr.net
** Ilona Petryk, Doctor of Economics, Lviv University of Business and Law, Lviv, Ukraine.

Ukraine in recent years, the number of recorded traffic accidents and the importance of ensuring the safety of transportation are presented.

ARTICLE INFO

Article history
Received: 30.09.2018 Accepted: 4.04.2019

Keywords
cargo transportation, safety, risks, supply chain, GPS

Introduction

Transport companies provide cargo transportation services to meet the needs of the national economy and those of the private sector of the country as well as to enable transit traffic through the country. Due to the transportation process, producers are connected with consumers and cargo. Also, national and interstate trade, both in raw materials and in finished products, is made possible due to transport. The efficient functioning of the transport sector contributes to the rise in the standard of living of the population and to the strengthening of the country's defense capability. A survey of enterprises providing freight transportation services was carried out on the issue of transportation safety. The survey was attended by 96 enterprises, mainly representatives of small and medium businesses.

Management of transportation risks in Ukraine

Cargo transportation is a business process that requires a responsible attitude, since its main purpose is to deliver goods safely to the place of destination. Guaranteeing safety – the absence of losses during transportation – is a vital task of transport and logistics companies, which select the most secure mode of transportation, taking into account a range of parameters, including the type of goods, conditions and ways of carriage.

Risk management in a transport company is a set of methods, techniques and measures that allow to predict to some extent the occurrence of risky events while carriage and to take measures to reduce them for saving money and time. Therefore, the process of risk management in an enterprise that delivers goods is expected to be carried out in a consistent way, starting with preparation of transport and transporting goods, and finishing with shipment of goods.

In general, in Ukraine every year an average of 7 thousand are killed in accidents and injuries of various degrees of severity happen to 57 thousand people. The consequences of accidents are hard. A separate factor of risk is the volume of the truck parking. The number of vehicles in Ukraine currently exceeds 9 million. The bulk of commercial vehicles, namely trucks and buses, has now moved to private ownership. As a result, the national level of provision of maintenance conditions and traffic safety has been destroyed, and the decisive criterion is profit, usually gained by violating the legislation and traffic safety requirements. The presence on the market of transport services of almost 15 thousand automobile carriers, who do not have the specialized education and experience of organization of transportation, also considerably worsens road safety.[1]

An insufficient level of road safety in Ukraine remains a serious problem. Thus, according to statistics for 2018, 217 accidents occurred on the roads of Ukraine due to drivers of licensed road transport, in which 33 people died and 536 were injured to varying degrees of gravity (208 accidents happened in the same period in 2017, in which 85 people were killed and 504 got injured). 191 accidents occurred due to the drivers of the buses, in which 29 people were killed and 498 got injured. Already this year, there were 43 accidents, in which 15 people were killed and 119 were injured (for the same period in 2017, there were 40 accidents in which 10 people were killed and 115 injured).[2]

In the territory of Ukraine over 1000 types of various dangerous goods is transported. In a country where military action is taking place, knowledge of the handling of dangerous goods and the legislative regulation of this aspect of transport activity is not a merely formal, but a vital need. Thus, according to statistics, only in 2018 there were 33 emergencies during the transport of dangerous goods, as a result of which the natural environment was "enriched" by 134 tons of industrial waste – chemicals, toxic substances, etc. Fortunately, it passed without sacrifices.

Over the past years there have been more massive catastrophes. An example is a catastrophe in the Lviv region in 2007 when 15 cisterns with yellow phosphorus got off the rail track. Then a fire began, during which

[1] National Department of Transport in Ukraine, *Motor vehicle traffic crashes as a leading cause of death*, "Annual Report of the Department of Transportation", 2019, pp. 43–48.

[2] National Department of Statistics in Ukraine, *Vantazhooborot ta obsyagi perevezen' vantazhiv u sichni-lystopadi*, http://www.ukrstat.gov.ua/operativ/operativ2018/tr/vp/vp_u/vp1118_u.htm (accessed: 1.03.2019).

a cloud of combustion products formed (the damage zone was about 90 square kilometers), and people from the nearest villages had to be evacuated. Due to poisoning with combustion products, 13 people in a state of high or moderate severity were hospitalized. Indeed, in the most industrially developed member states of the European Union, the share of dangerous goods transportation is about 20% of the total volume of transport, of which almost 40% is for flammable liquids (in particular, fuel).

The acknowledgement of the European experience may be the adoption of Draft Law # 7387 "On Amendments to Some Laws of Ukraine on bringing them in line with the legislation of the European Union in the field of transportation of dangerous goods". It was included on the Council's agenda at the end of March, after the previous law, registered back in 2016, with the same name and in fact the same bill, which was not adopted at the second reading.

The stages of transport risk management in Ukraine

To commence the process of risk management in transportation, one must identify the external and internal risks of the logistics system under study. Each supply chain and each logistics system – or even a single fraction thereof – has its own risk system, whose characteristics depend on the logistic functions performed (transportation, warehousing, purchasing management, etc.), industry affiliation, scale of activity (local, regional, national, international, global), technologies, development strategies and a number of other factors. While identifying company risks, first of all, one should detect all types of risk that are specific to this enterprise.

According to the survey of transport enterprises, the following types of risks which transport enterprises confront in Ukraine can be distinguished:

1. Managerial – risks related to documentation (no application for transport services for transportation, no necessary documents for the carriage of dangerous goods, no necessary documents for the moment of transportation to the driver of a tanker truck; risks associated with marking; incompleteness and insufficiency of cargo information); transport risks (incorrect definition of the moment of transfer of responsibility for the cargo in the process of transportation, the risk of choosing a vehicle, the risk of poor quality cargo, uncoordinated time of shipment, uncoordinated itinerary of loading and unloading of the tanker, uncoordinated transportation route); personnel risks (the risk of cargo damage during

transportation, low level of skills of employees, failure of the employee to fulfill their job duties).
2. Technical – risks associated with the operation of technical equipment in the logistics system, the risk of differences in the weight indices of the load at the entrance and exit of the vehicle.
3. Unplanned – risk of theft of goods; risk of an accident; natural disasters; damage to cargo; loss of cargo due to overloading.
4. Commercial – failure of supply; lack of production; violation of delivery terms.
5. Unpunctuality-related – the risk of cargo delay during transportation; the risk of delaying the unloading of the tanker.
6. Entrepreneurial – change of contractual conditions by the customer of transportation; liquidation of the enterprise.
7. Depreciation – rapid physical wear of transport and equipment; outdated transport and equipment.
8. Financial – the risk of inflation; fluctuations in exchange rates.

Then, qualitative and quantitative risk assessment is carried out. The mere detection of logistic and non-logistic risks appropriate to an enterprise do not make it possible to identify the dangers that they represent and to choose the risk management procedures that will most effectively counteract them. To solve such problems, it is necessary to estimate the size of possible losses resulting from those risks, and the probability of their occurrence. The main task of qualitative assessment is to obtain information on the structure and the properties of the logistics system and its inherent risks, and to identify the factors and circumstances leading to these risks. Quantitative assessment allows one to get the numerical value of the risks inherent in the logistic system of the enterprise, to find out about the probabilities of their occurrence and to obtain the prognosis on their consequences. At this stage, risk assessment methods such as the statistical method, the expert estimation method or the analogue method can be used. The essence of statistical methods for assessing transport risk is to determine the probability of occurrence of losses in transportation on the basis of statistical data of the previous period and the establishment of a risk zone, risk factor, etc. Often, as a characteristic in the methods of statistical risk assessment, the variance and standard deviation, coefficient of variation is used. The essence of the method of expert assessments of transport risks is the rational organization of expert analysis of the problem during transportation with the quantitative assessment of judgments and the processing of their results.

Summarized expert opinions are considered as a solution to a specific problem. Analogue methods are used for the identification of potential risk factors during transportation, based on previous transportation experience.[3]

What is important is the further diagnosis of risks. It involves the analysis of the impact of risk factors on logistic performance indicators. These analytical measurements are carried out using such tools as correlation, regression analysis methods, or expert assessments. In correlation certain risk factors for transport are exposed to stress-relief, while others vary according to their correlation under normal conditions. Regression analysis is to determine, basing on experimental data, of the coefficients of the model (regression coefficients), and to assess the significance of the values of these coefficients and the degree of the adequacy of the model. Expert assessments allow, by summarizing the experts' opinion about the probability of losses during transportation, to obtain the amount of acceptable risk or the loss magnitude.

Another step in risk management process is the prediction and the modelling of the outcome of the risk and of the consequences of the decisions made. This stage involves the use of tools such as the decision tree, method of analysis of danger and efficiency, or analysis of scenarios. Decision tree method is a situational analysis method, the essence of which is the process of making managerial decisions in terms of assessing the level of risk of a project that arises as a result of the carriage process implementation. The method of analysis of danger and efficiency is about the study of the impact of technological parameters (temperature, pressure, etc.), as well as deviations from regulated regimes in terms of danger. Analysis of scenarios for the development of project transport allows one to assess the impact on the project of the possible simultaneous change of several factors depending on the probability of each scenario. The next step – the assessment of risk acceptability – is to make one realize that in most cases it is not possible to completely get rid of the risk, which can only be reduced to an acceptable level at which it ceases to be dangerous.[4]

[3] A. Mehrara Molan, M. Rezapour, K. Ksaibati, *Modeling the impact of various variables on severity of crashes involving traffic barriers*, "Journal of Transportation Safety & Security", 2 March 2019, pp. 800–817, https://doi.org/10.1080/19439962.2018.1547995.

[4] A. Thankappan, L. Vanajakshi, *Development and application of a traffic stream model under heterogeneous traffic conditions*, " Journal of The Institution of Engineers (India): Series A", vol. 96, issue 4, pp. 267–275, https://doi.org/10.1007/s40030-015-0134-y.

Finally, there is the choice of an appropriate method for managing the risk of the logistics activities of an enterprise. Such methods in the practice of enterprise management often are: preventive measures to reduce the risk, transfer of risks, external insurance, or the refusal of risk. These methods allow to minimize the risk directly affecting the transport company and share some part of responsibility with another subject.

Safety of cargo transportation in Ukraine

Cargo damage in transportation (loss of merchantability or the deterioration of cargo properties) and cargo theft are examples of the risks confronted by transport companies. However, modern logistics develops a range of methods and means of ensuring the safety of freight traffic.

When it comes to counteracting cargo damage, one of the methods is to design pre-drawn schemes for the correct loading and placement of goods in the vehicle, as well as the use of modern fastening elements that prevent the displacement of goods during transport. Only 30 percent of the companies surveyed in Ukraine develop the above schemes.[5] This issue is not a big deal, as companies believe that classical schemes that were developed in the beginning of the century, or even in the Soviet period, are universal and suitable for each type of transportation. Enterprises that develop such schemes do not attach much importance to this issue either, though on average they allocate 10 percent of the cost to this purpose. Another method of preventing such damage is the provision of additional fillings. In Ukraine, this method is more popular than the previous one, but also not very common. Among the respondents, 40 percent use it. The reason other companies do not use it are additional costs connected with the content. For companies with a limited budget, it is important to use existing transportation facilities without extra cost.

As regards the prevention of theft, available methods involve the employment of armed guards, the use of GPS satellite tracking, the involvement of independent observers, and additional insurance. Each of these methods has its own specificity and fields of application. For example, it is expedient to decide for the expensive maintenance of armed security only during the transportation of particularly valuable and excisable goods to reduce

[5] B. Heydecker, J. Addison, *Analysis and modelling of traffic flow under variable speed limits*, "Transport Research Part C: Emerging Technologies", 2018, no. 19(2), pp. 206–217, https://doi.org/10.1016/j.trc.2010.05.008.

the risk of theft considerably. Therefore, only 5 percent of the enterprises surveyed incorporate armed security in the budget expenditures, since this method is rather expensive and may even consume 40 percent of the budget. 5 percent enterprises which implement this method of cargo protection are, basically, engaged in the transportation of highly financially assessed cargo. The use of satellite control systems to monitor vehicles with cargo is becoming more and more widespread. It allows to record the vehicle's stops on the road, planned or unplanned; and certain systems, owing to special sensors, prevent the vehicle from becoming subject to unauthorized entry. Therefore, more than 55 percent of surveyed carriers use GPS in their work, since they believe that this method helps to optimize time and money. The remaining respondents which could not afford to include it in the budget due to lack of funds, do not use this method.[6]

The involvement of independent observers to guard transported cargo has become increasingly popular in recent years and is widely used by transport carriers is the whole world. The participation of independent observers in the processes of loading and unloading of industrial goods in transshipment warehouses often disciplines cargo carriers as well as the senders and the recipients of the cargo, forcing them to treat their contractual obligations in a responsible way. Unfortunately, the involvement of independent observers in Ukraine is quite rare, as shown by the survey conducted. Only 7 percent of respondents use this method; thus, its popularity is similar to the popularity of armed security hiring. Involving an independent observer in Ukraine is expensive, therefore, firms generally consider this method unprofitable, that is, a waste of money.[7]

The safety of dangerous and oversized loads transported in Ukraine

A proper supply chain is not only about delivering fast but also about delivering safely and in compliance with international standards. This is especially important when it comes to dangerous goods such as petroleum products, fertilizers, cement, pesticides, etc. Dangerous loads, which often have a form of e.g. flammable liquids or toxic or explosive substances, can cause harm to humans and/or the environment when they evaporate, leak, or

[6] E. Hauer, *The art of regression modeling in road safety*, Berlin 2017, p. 38.

[7] M. Rezapour, P. Saha, K. Ksaibati, *Impact of traffic enforcement on traffic safety*, "International Journal of Police Science and Management", 2017, vol. 19, issue 4, https://doi.org/10.1177/1461355717730836, p. 268.

crumble during transportation. Therefore, avoidance of accidents involving such loads is particularly important within the area of load safety.

Road transport of oversized loads, despite its highest popularity, is struggling with the greatest number of problems, mainly related to technical and legal obstacles occurring on the transport route from the place of shipment to the destination.[8]

Today, in Ukraine, regulatory documents provide for the carriage of goods with a total mass (including the mass of the vehicle) no more than 40 tons. The above norm does not differ from the European one. On an exceptional basis, for container vehicles it is 44 tons, and for vehicles moving on special routes established by Ukravtodor and corresponding units of the Ministry of Internal Affairs it is up to 46 tons. Besides, weights are controlled as regards axle load: the amount of loading on a single axle – 11 tons, for double loads – 16 tons, for the building – 22 tons. According to data provided by the State Dignity Institute, about 74% of highways were constructed under the estimated load on the axle totalling 6 tons and the total weight not exceeding 24 tons.

The annual losses incurred by the road economy because of the destruction of roads caused by the traffic of heavy vehicles exceed 2 billion UAH. According to World Bank studies, annual losses of the country's GDP due to unsatisfactory state of highways comprise 3–4% of GDP. More than 90% of highways in Ukraine are in need of repair and construction work.[9]

The route planning process in transporting oversize loads usually takes into account road conditions such as the assessment of the width of roads, the turning radius, the existing signs and poles, the height and width of trips under overpasses and bridges and the permissible load of bridges and viaducts; the occurrence of the elements of infrastructure such as roundabouts, pedestrian crossings and islands; the allowed pressure on the surface; as well as the location of electric tractions, railway tractions, road repairs etc. There is a frequent need to remove road obstacles for the time of the passage of an oversized transport vehicle. It happens that the distance between the point of sending and the destination is small; however, to carry a given element,

[8] S. Nama, A. Maurya, A. Maji, *Vehicle speed characteristics and alignment design consistency for mountainous roads*, "Transportation in Developing Economies", 2018, no. 2(2), 23, https://doi.org/10.1007/s40890-016-0028-3, p. 23.

[9] National Department of Statistics in Ukraine, *Vantazhooborot…*, *op. cit.*

a much greater distance should be covered. As a result, the recipient pays more for transportation, while the time of carriage lengthens.[10]

In order to preserve the roads of general use, there is a central executive body: Ukrtranssabspekta, which is responsible, in particular, for the implementation of dimensional and weight control over vehicles as well as dimensional and weight parameters that exceed the normative ones, and for the measures to prevent and avoid the destruction of highways.

The implementation of the overall and weight control of vehicles is regulated by:

- Law of Ukraine "On Automobile Transport";
- Law of Ukraine "On Road Traffic";
- Rules of the Road, approved by the Cabinet of Ministers on 10 October 2001 (as amended);
- The Resolution of the Cabinet of Ministers of 27 June 2007 no. 879 "On Measures for the Safekeeping of Motorways of the Common Use".

At this time, the territorial bodies of Ukrainian transport safety, together with the services of motor roads in the regions and relevant units of the National Police of Ukraine in districts, started to carry out measures on dimensional and weight control using mobile weight machines and weight systems.

As a result of their work, 4,556 vehicles have already been checked, of which 319 revealed a violation of weight parameters. The travel fare is charged of 150 thousand UAH. Penalties amounting to about 148 thousand UAH were imposed.

The first step in the planning of the logistics chain in oversized load transport is the analysis and the assessment of the transport's capability. Legal requirements are to be met and necessary permits must be obtained that allow the carriage of oversized cargo on public roads. An important factor conditioning the safety of oversize cargo transportation is the coordinated work of qualified staff and effective communication among them. Another important step of the aforementioned process is the reliable planning of the transport route that minimizes the risk for both people involved in the carriage and the environment. Adequate marking and lighting of the load is another factor important for maintaining safety in this type of transport. Another factor is compliance with permits and recommendations pertaining to the carriage of a given load along a given route, as well

[10] M. Rezapour, S. Wulff, K. Ksaibati, *Impact…*, *op. cit.*

as possession of necessary documents by the driver.[11] Another action aimed at maintaining safe transportation of oversized cargo is the preparation of the load by guaranteeing relevant means of protection (checking the state of the equipment, e.g. hooks or tension belts; ensuring the appropriate distribution of the load on the trailer, etc.). To transport an oversized load, one also needs specialized vehicles, selected and adjusted to manage the transported cargo. Final points concerning the safety of oversized transport are ensuring that the means of transport will not be damaged by the weight of the load, and that the transportation processes performed by other road users will not be hampered.

Conclusions

Nowadays the carriage of dangerous goods in Ukraine is regulated by the law "On the Transport of Dangerous Goods", as well as laws on certain types of transport, Government acts, and orders of the Ministry of Infrastructure and the Ministry of Internal Affairs.

By concluding the Association Agreement with the European Union, Ukraine has undertaken to harmonize existing transport standards with those prevailing in the EU, in particular with Directive 2008/68/EC on the internal carriage of dangerous goods, which actually extends international agreements on dangerous goods for domestic transport. In 2015, the Ministry of Infrastructure together with the Ministry of Internal Affairs met the European requirements by approving the "Procedure for inspection of tanks for the transport of dangerous goods", and afterwards adopting the rules for the carriage of dangerous goods by inland waterways of Ukraine.

The main shortcomings of the current legislation that regulates the process of transporting dangerous goods is the inconsistencies in the legal documents and the discordance between them, as well as the non-compliance with the norms of technical progress. For example, in the law "On the Transport of Dangerous Goods", there is no list of vehicles intended for the carriage of such cargoes. Thus, the requirements regarding the condition, design, or equipment of such vehicles are also absent.

Also, domestic law does not regulate the procedure for resolving disputes related to the transport of dangerous goods, as well as the procedure

[11] J. Piao, M. McDonald, N. Hounsell, M. Graindorge, T. Graindorge, N. Malhene, *Public views towards implementation of automated vehicles in urban areas*, "Transportation Research Procedia", 2016, vol. 14, pp. 2168–2177, http://www.sciencedirect.com/science/article/pii/S2352146516302356 (accessed: 3.03.2019).

for monitoring compliance with the requirements for carriage; there is no answer to the question of who should be responsible for controlling the transportation of dangerous goods at different stages of transportation.

The current situation of freight transport security in Ukraine does not meet the expectations of society; it leads to numerous human, material and economic losses, while creating social tension in the state and unfavorable conditions for investment in the transport sector of Ukraine. A possible solution to this problem would be e.g. the introduction of an effective state system of control in compliance with transport companies operating and rest regimes, as well as improving the requirements regarding the safety level of the design of vehicles.

References

1. Hauer E., *The art of regression modeling in road safety*, Berlin 2017.
2. Heydecker B., Addison J., *Analysis and modelling of traffic flow under variable speed limits*, "Transport Research Part C: Emerging Technologies", 2018, no. 19(2), pp. 206–217, https://doi.org/10.1016/j.trc.2010.05.008.
3. Mehrara Molan A., Rezapour M., Ksaibati K., *Modeling the impact of various variables on severity of crashes involving traffic barriers*, "Journal of Transportation Safety & Security", 2 March 2019, pp. 800–817, https://doi.org/10.1080/19439962.2018.1547995.
4. Nama S., Maurya A., Maji A., *Vehicle speed characteristics and alignment design consistency for mountainous roads*, "Transportation in Developing Economies", 2018, no. 2(2), 23, https://doi.org/10.1007/s40890-016-0028-3.
5. National Department of Statistics in Ukraine, *Vantazhooborot ta obsyagi perevezen' vantazhiv u sichni-lystopadi*, http://www.ukrstat.gov.ua/operativ/operativ2018/tr/vp/vp_u/vp1118_u.htm (accessed: 1.03.2019).
6. National Department of Transport in Ukraine, *Motor vehicle traffic crashes as a leading cause of death*, "Annual Report of the Department of Transportation", 2019, pp. 43–48.
7. Piao J., McDonald M., Hounsell N., Graindorge M., Graindorge T., Malhene N., *Public views towards implementation of automated vehicles in urban areas*, "Transportation Research Procedia", 2016, vol. 14, pp. 2168–2177, http://www.sciencedirect.com/science/article/pii/S2352146516302356 (accessed: 3.03.2019).
8. Rezapour M., Saha P., Ksaibati K., *Impact of traffic enforcement on traffic safety*, "International Journal of Police Science and Management", 2017, vol. 19, issue 4, pp. 238–246, https://doi.org/10.1177/1461355717730836.

9. Rezapour M., Wulff S.S., Ksaibati K., *Predicting truck at-fault crashes using crash and traffic offence data*, "The Open Transportation Journal", 2018, vol. 12, pp. 128–138, https://doi.org/10.2174/1874447801812010012 8.
10. Thankappan A., Vanajakshi L., *Development and application of a traffic stream model under heterogeneous traffic conditions*, " Journal of The Institution of Engineers (India): Series A", vol. 96, issue 4, pp. 267–275, https://doi.org/10.1007/s40030-015-0134-y.

cite this article as:
L. Yankovska, I. Petryk, *Safe transportation of goods in the supply chain of contemporary Ukraine: risk management and means of loading safety*, [in:] *Security in Central and Eastern Europe: Cyberspace, Police, Prisons, Transport, Addictions, the Media. Proceedings from the Conference XLIV CICA: "Security in Europe" – 12th Security Forum Krakow, 5–7 June 2018, Kraków, Poland*, Krakow 2020, pp. 106–118, https://doi.org/10.24356/proceedings2018/5.

INDIVIDUAL SECURITY IN POLAND AND EUROPE

**SECURITY IN CENTRAL AND EASTERN EUROPE:
CYBERSPACE, POLICE, PRISONS, TRANSPORT, ADDICTIONS, THE MEDIA**
Proceedings from the Conference
XLIV CICA: "Security in Europe" – 12th Security Forum Krakow
5–7 June 2018, Kraków, Poland
2020 (120–133); https://doi.org/10.24356/proceedings2018/6

Why Doesn't Prevention Work? Drug and Alcohol Prevention among Adolescents in Europe

Marzanna Farnicka*

ABSTRACT

Alcohol is one of the main determinants of health problems related to lifestyle, especially in Europe. Because of related health problems and negative social impacts, including violence, hooliganism and family problems, the use of drugs and alcohol is monitored by the EU. According to the European Monitoring Centre for Drugs and Drug Addiction,[1] addiction treatment and the results of obligatory prevention programmes are different in various countries in Europe. The article presents factors connected with unsuccessful prevention programmes from the European perspective based on the data from the European School

* Marzanna Farnicka, Ph.D., University of Zielona Góra, Zielona Góra, Poland; correspondence address: Instytut Psychologii, Uniwersytet Zielonogórski, al. Wojska Polskiego 69, 65-762 Zielona Góra, Poland; email: m.farnicka@wpps.uz.zgora.pl

[1] European Monitoring Centre for Drugs and Drug Addiction, *European Drug Report*, Luxembourg 2016, http://www.emcdda.europa.eu/edr2016_en (accessed 10.07.2018).

Survey Project on Alcohol and Other Drugs.[2] Special attention is paid to the results obtained in Poland, because, according to the survey carried out in 2015, the use of drugs in Poland increased in comparison with 2011. The causes of European diversity in using drugs among adolescents are discussed from the contextual perspective. Factors were analyzed in different type of context including: law regulations, family attitudes, peers influences and accessibility of drugs.

ARTICLE INFO

Article history
Received: 30.09.2018 Accepted: 4.04.2019

Keywords
adolescents, drugs, family factors, prevention programmes, values

Introduction

Europe is the continent where alcohol consumption per capita is the highest in the world.[3] In established market economies, such as the EU Member States, the burden of alcohol-related diseases and harm is estimated at 8 to 10%. For this reason, the prevention of harmful and dangerous consequences of alcohol consumption is a priority for public health in many Member States of the European Union and the rest of the world. The World Health Organization[4] forecasts that by 2025 alcohol per capita consumption (15+ years) will have risen globally despite the expected decrease in alcohol consumption in the WHO European Region (by 0.6 litres per capita). The European Monitoring Centre for Drugs and Drug Addiction (EMCDDA) since 2007 regularly carries out the survey on the changes in the use of various drugs among adolescents in Europe. The results show that there has been an increase in drug production, and a range of drug substances has become wider. Moreover, new problems have emerged including new syn-

[2] European Monitoring Centre for Drugs and Drug Addiction, *European Drug Report*, Luxembourg 2015, http://www.emcdda.europa.eu/edr2015 (accessed 16.08.2018).

[3] WHO, *World Health Organization Report Substance Abuse*, 2014, http://www.who.int/substance_abuse/publications/global_alcohol_report/msb_gsr_2014_1.pdf?ua=1 (accessed 10.08.2018).

[4] *Ibidem*.

thetic cannabis, the Internet market (darknet), or new forms of addiction.[5] The WHO report also shows that Europe has its own diversity in the use and consequences of drugs and alcohol. Although the highest alcohol-attributable fractions (AAF) are reported in the WHO European Region, the high result is almost entirely driven by Eastern European countries.[6] It is worth noticing that more risky patterns of consumption, that are usually observed in less wealthy countries, do not exist in Eastern Europe. There is higher disease burden per liter consumed than it might be expected from the economic development.[7]

Facts on alcohol and drugs use among youth in Europe

Research on the quality of treatment and prevention started many years ago. Zimberg (1999) was one of the researchers who were disappointed with the state of addiction treatment and prevention. In his works Zimberg presented an integrative perspective to addiction diagnosis and treatment. According to this old classification, it is very important to recognize the second type of addiction, where an individual has problems with mental health as a consequence of using a substance.[8]

In this article, the starting point for analyzing the problem of the use of alcohol and drugs among adolescents was the European School Survey Project on Alcohol and Other Drugs.[9] The survey was conducted in six waves of data collection, with 1995 as the starting point. The study showed that in 22 countries the lifetime uses of cannabis peaked in 2003 and then slightly decreased in the 2007 survey. Since then, the prevalence has been

[5] European Monitoring Centre for Drugs and Drug Addiction, *European Drug Report*, Luxembourg 2017, http://www.emcdda.europa.eu/system/files/publications/4541/TDAT17001ENN.pdf (accessed 10.08.2018); European Monitoring Centre for Drugs and Drug Addiction, European Drug Report, Luxembourg 2018, http://www.emcdda.europa.eu/system/files/publications/8585/20181816_TDAT18001ENN_PDF.pdf (accessed 12.08.2018).

[6] WHO, *Global status report on alcohol and health – 2014*, 2014, https://apps.who.int/iris/bitstream/handle/10665/112736/9789240692763_eng.pdf;jsessionid=48A9543F4F28A8DE11B0342AE3447148?sequence=1 (accessed 10.07.2018).

[7] *Ibidem*.

[8] S. Zimberg, *A dual diagnosis typology to improve diagnosis and treatment of dual disorder patients*, "Journal of Psychoactive Drugs", 1999, no. 31(1), pp. 47–51, https://doi.org/10.1080/02791072.1999.10471725.

[9] *The European School Survey Project on Alcohol and other Drugs*, 2015, http://www.espad.org/report/home (accessed 16.08.2018).

relatively stable. The long-term lifetime use of inhalants has been relatively stable as well. For sedatives and tranquilisers, lifetime use decreased slightly between 1995 and 2015, with consistently higher prevalence of use among girls than among boys over this period.

The 2015 ESPAD Report[10] collected comparable data on substance use among 15- to 16-year-old students from 35 European countries, including 23 EU Member States and Norway.

The data reveal some diversity across Europe. The 2015 results show that:

- among students in these 24 countries, on average, 18% reported having used cannabis at least once (lifetime prevalence), the highest levels reported by the Czech Republic (37%) and France (31%),
- among students in these 24 countries, on average 8% reported having used cannabis in the last 30 days,
- the use of illicit drugs other than cannabis (MDMA/ecstasy, amphetamine, cocaine, methamphetamine and hallucinogens) was far lower, with an overall lifetime prevalence of 5%,
- the average lifetime prevalence of the use of inhalants was 8% (ranging from 3% in Belgium (Flanders) to 25% in Croatia),
- lifetime use of sedatives or tranquilisers without a doctor's prescription was reported by an average of 6% of students (ranging from 2% in Romania to 17% in Poland),
- lifetime use of new psychoactive substances was reported by an average of 4% of students (ranging from 1% in Belgium (Flanders) to 10% in Estonia and Poland),
- new psychoactive substances have been used during the last 12 months by 3.2% of participants (herbal smoking mixtures were the most commonly used type of substance – 2.6% of all participants).

The above results are intriguing. Why are anti-alcohol and anti-drugs programmes, which have been implemented at high costs on various (EU, national and local) levels to reduce alcohol-related harm, ineffective? According to the Report prepared by the Consortium for DG Health and Consumers (COWI) of the European Commission[11] just in the period between 2007 and 2012, 9 million euros were spent on anti-alcohol pro-

[10] *Ibidem*.

[11] *Assessment of the added value of the EU strategy to support Member States in reducing alcohol-related harm*, December 2012, https://ec.europa.eu/health/sites/health/files/alcohol/docs/report_assessment_eu_alcohol_strategy_2012_en.pdf

jects and approximately 49 million euros were given to studies on alcohol and health.[12]

Success of treatment and prevention – factors

The word *prevention* usually means activities that stop an action or behavior. It can also be used to depict activities that promote a positive action or behavior. Research has found that successful prevention models and programs must include both: reduce risk factors and promote protective factors to ensure the goals. This article discusses factors hidden in social and cultural background that make the results of programmes, social policy and health care not predictable enough to prevent or effectively reverse the problems. They are discussed below from the contextual perspective.[13] According to these assumptions the development environment consists of: **macro-system** (law regulation and institutional care), **ecosystem** (accessibility of drugs, school culture), **meso-system** (peers and parental values and attitudes) and **micro-system** (individual factors).

Factors hidden in the macro-system (law regulation and institutional care)

In many European countries, the concept of alcohol-free upbringing and counteracting alcoholism is regulated in different ways. However, usually the framework is quite similar; it usually includes e.g. the protection of children and adolescents, a lot of prevention programmes, and the treatment of addiction which has a voluntary character except the cases when the court orders the person to treat addiction.[14] The treatment of drug-related disorders is free of charge for adolescents and in many countries also for those who have no social insurance.

But there are also a lot of differences among the European Union (EU) countries. There are different lists of forbidden drugs, different legal drinking ages (between 16 and 18), semi-prohibition, special shops and pubs, as well as special rules concerning the use of alcohol and other substances in public places. The law of a particular country makes a certain climate

[12] T. Zamparutti *et al.*, *Assessing and strengthening the science and EU environment policy interface*, "European Commission Technical Report", pp. 2012–2059, https://doi.org/10.2779/1028.

[13] U. Bronfenbrenner, *Making Human Beings Human Bioecological Perspectives on Human Development*, Thousand Oaks, CA 2005.

[14] T. Zamparutti *et. al.*, *Assessing…*, *op.cit.*

and creates a certain system of thinking about health problems and state responsibility for adolescents.

Therefore, analysing the differences in prevention systems, it is impossible to ignore the level of economic development of a given society, which determines a given model of interactions as the most suited to its capabilities and resources. The analyses of the relations between the prevention systems and the model of legal tradition in a given country (caring model, juridical model, participatory model, the model of restorative justice) were done e.g. by Gupta and Smith,[15] and Kusztal.[16]

In the EU countries there are different assumptions on the role and responsibility of the family and the state in terms of the goals and methods of socialization.[17] In the **"protective systems"** (e.g. in Scandinavia, Germany), government institutions are partners with parents and school in solving problems. They can affect parental care, teach parents if necessary, or provide parental monitoring. In **"preventive systems"** the family functions as an independent entity that is loosely connected to the network of state institutions. Only a clear law violation that is an offence prosecuted ex officio, or an offence against a given person (family member), makes the institution pay attention to the family (e.g. in Poland, Great Britain). This means that parents are the main subjects to decide about their child/children. School and government institutions can only intervene when necessary, that is when the child or adolescent has problems with law documented by the police. Obviously, there are some system approaches to taking care of children and adolescents in schools, but the strength of their influence on family as a whole varies.[18]

[15] N. Gupta, N. Smith, V. Mette, *Child Care and Parental Leave in the Nordic Countries: A Model to Aspire to?*, "IZA Discussion Paper", 2006, no. 2014, https://ssrn.com/abstract=890298 (accessed 5.09.2018).

[16] J. Kusztal, *Europejskie tendencje w zapobieganiu przestępczości nieletnich*, "Probacja", 2011, no. 4, pp. 33–34.

[17] *Brussels IIa Regulation 2201/2003*, https://www.peacepalacelibrary.nl/plinklet/?sid=bloginfo&ppn=263129977 (accessed 13.08.2018); M. Farnicka, M. Kuźmik, *Rola Rodziny w systemie resocjalizacji i profilaktyki społecznej w różnych krajach europejskich i pozaeuropejskich*, [in:] *Teoretyczne i praktyczne aspekty funkcjonowania młodzieżowych ośrodków wychowawczych*, G. Miłkowska, E. Magda (eds), Zielona Góra 2016, pp. 47–64.

[18] K. Boele-Woelki, *What Family Law for Europe?*, "Rabels Zeitschrift fur auslandisches und internationales Privatrecht" [The Rabel Journal of Comparative and International Private Law], 2018, vol. 82 (1), pp. 1–30.

Factors hidden in the ecosystem (peer influence, school influence, accessibility of drugs)

Studies show that there is **high availability** of psychoactive substances to adolescents. Despite numerous measures, the vast majority of adolescents – 60% of 15-year-olds and over 80% of 17-year-olds – claim that acquiring alcohol is very easy. The majority of respondents have smoking experience, and around 3% of junior high school students and 6% of high school students smoke more than 10 cigarettes a day (results were recorded in Poland; according to the survey carried out in 2015, Polish adolescents were still highly at risk for legal psychoactive substances (the figures increased in comparison with 2011).

Another risk factor for the psychoactive substances demand is being involved in the circles of substance users. If one's social contacts are limited to people who smoke tobacco, drink alcohol or use drugs, the risk of adopting these behaviour patterns is quite high. And the most "first time" uses occurred among peers during breaks or holidays and at parties or meetings. Adolescents stressed their expected cultural patterns of behaviour**,** which were far from the standards of abstinence and responsibility.

As an illustration, one example can be presented. In Poland, Polish Agency for Solving Alcohol Problems (PARPA) coordinates the functioning of the system of addiction prevention and treatment.[19] The Agency addresses preventive actions for individuals – children and adolescents as well as adults. The Agency conducted a survey on the attitudes to the possible introduction of the sellers' joint responsibility for damages caused by a drunken minor whom they have sold alcohol. The survey was addressed to adolescents and adults. The study group consisted of 500,000 adolescents, and 43,000 adults. The results of the survey have shown that 80% (400,000) of adolescents agreed that such responsibility should be assigned. In turn, in adults group 36,000 persons agreed, which was 84% of the group. So the result is maybe the answer to the question what adolescents think about the responsibility for their own lives.

Factors hidden in the mezo-system (family impact, parental values and attitudes)

The analysis of the literature describing the importance of the family in the child and youth development leads to two conclusions: firstly, parent-child

[19] PARPA, *Kampanie profilaktyczno-edukacyjne*, http://www.parpa.pl/index.php/profilaktyka-system-rekomendacji/kampanie-profilaktyczno-edukacyjne (accessed 5.09.2018).

interaction is determined by two main dimensions of parenting, i.e. caring, that is, warmth and support, and control, i.e. supervision and discipline; secondly, family variables, such as: parents' dispositions, their mutual relations, relationships with siblings, and the socio-cultural context in which the family functions, determine the interaction between the parent and the child. Empirical studies prove that parents-alcoholics and parents-non-alcoholics differ in the scope of performing parental functions, especially in providing support to children and control.[20] On the one hand, the children of parents-alcoholics are a risk group prone to develop mental disorders in terms of the intensity of various symptoms. The risk results from greater psychological susceptibility of the children of alcoholics to developmental problems and the specificity of their developmental context. On the other hand, the study carried out by Grzegorzewska[21] confirmed that not all children of alcoholics found it difficult to adapt to social requirements. Some of them (about 40%) coped well with developmental tasks and despite many negative, often accumulated, traumatic events, they could find joy, satisfaction and contentment in life. It remains unclear whether the greater risk is a direct result of the impact of alcoholism, or an intermediate product of genetic and environmental influences, including loose family bonds, poor physical and emotional availability of parents, decreased quality of parental functions, or the generally nervous and unstable atmosphere of everyday life, filled with conflicts.

A family history of alcohol use disorders is considered a major vulnerability factor for both genetic and environmental reasons.[22] Heritable or genetic risk factors account for a substantial proportion of the variation in alcohol dependence. Multiple genes influence such features as alcohol use initiation, its metabolism and reinforcing properties in different ways, contributing to the increased susceptibility to the toxic, psychoactive and dependence-producing properties of alcohol in some vulnerable groups and individuals. Parental alcohol use disorders have been found to negatively affect the family situation during childhood. Parents with alcohol use disorders display particular patterns of alcohol consumption and thereby increase the likelihood that their children will develop drinking patterns

[20] J.E. Kim, E.M. Hetherington, D. Reiss, *Associations among family relationships, antisocial peers, and adolescents' externalizing behaviors: Gender and family type differences*, "Child Development", 1999, no. 70, pp. 1209–1230, https://doi.org/10.1111/1467-8624.00088.

[21] I. Grzegorzewska, *Dorastanie w rodzinach z problemem alkoholowym*, Warszawa 2011.

[22] WHO, *Global…*, *op.cit.*

associated with high risk of alcohol use disorders when they are introduced to alcohol.[23] Here the mechanism of intergenerational transmission should be mentioned. The studies in this area concern describing and emphasizing continuation (similarity) in family treated as an indicator of the transmission or parental attitudes.[24] There are also numerous studies concerning the similarity of values and expectations towards future. This aspect has been discussed by Gans and Silverstein.[25]

As the illustration of the mentioned problem, the result of ESPAD Report[26] is presented. Right attitudes are protective factors – i.e. those including lack of consent to drink alcoholic beverages or smoke cigarettes, at least before turning 18. Only slightly more than half (51%) of Polish 15-year-olds and 25% of 17-year-olds have this absolute ban from their parents. (For example 30% Polish parents accept drinking alcohol and smoking by their adolescent children but not in their presence, and 29% allow their teenage children to use substances during family events or peer meetings even when they are at home.) The research results indicate that parents need to be educated in this area and it is a potential factor protecting against the use of legal psychoactive substances.

Factors hidden in the micro-system

Children, adolescents and elderly people are typically more vulnerable to alcohol-related harm from a given volume of alcohol than other age groups.[27] Also, early initiation of alcohol use (before the age of 14) is a predictor of impaired health status because it is associated with an increased risk

[23] A. J. McFadden, M. Young, F. Markham, *Venue-Level Predictors of Alcohol-Related Violence: An Exploratory Study in Melbourne, Australia*, "International Journal of Mental Health and Addiction", 2015, no. 13, pp. 506–519, https://doi.org/10.1007/s11469-015-9552-3.

[24] T. Thornberry, A. Lizotte, M. Krohn, M. Farnworth, S. Jang, *Deliquent peers, beliefes and delinquent behavior: a longitudinal test of interactional theory*, "Criminology", 1994, no. 32, pp. 47–83, https://doi.org/10.1111/j.1745-9125.1994.tb01146.x.

[25] T. Thornberry, A. Freeman-Gallant, A. Lizotte, M. Krohn, C. Smith, *Linked lives: The Intergenerational Transmission of antisocial behavior*, "Journal of Abnormal Child Psychology", 2003, no. 31, pp.171–189.

[26] *The European School Survey Project on Alcohol and other Drugs*, *op. cit.*

[27] B. F. Grant, D.A. Dawson, *Age at onset of alcohol use and its association with DSM-IV alcohol abuse and dependence: results from the National Longitudinal Alcohol Epidemiologic Survey*, "Journal of Substance Abuse Treatment", 1997, no. 9, pp. 103–110, https://doi.org/10.1016/s0899-3289(97)90009-2.

of alcohol dependence and abuse at later ages.[28] At least part of the risk among young people is related to the fact that, typically, a greater proportion of the total alcohol intake by young people is consumed during heavy drinking episodes. Also, young people appear to be less risk-averse and may engage in more reckless behaviour while drunk. The second individual factor is related to the sex of a youth. Blatt-Eisengart, Drabick, Monahan and Steinberg presented the results of studies on sex and differences in susceptibility to family influence. Based on the longitudinal studies they formulated the concept that sex may be treated as a risk factor which provides for family transmission.[29] The next usually mentioned factor is a youth's style of attachment. There are many studies which confirmed this factor.[30]

Another more specific factor affecting behavior related to psychoactive substances is the **belief on health consequences** and other damages related to their use. It can be assumed that for the majority of young people, the conviction that substance use may be highly harmful will result in their avoidance, and the conviction about their harmlessness will be conducive to making decisions to use them. In this sense, these beliefs may constitute a risk factor or be a protective factor. Most teenagers who use psychoactive substances claim they cause little health damage. They also reveal positive expectations regarding the effects of these substances. Those who do not experiment with substances are convinced about their high harmfulness or addiction risk.[31]

Conclusion

Why doesn't prevention work? The already presented ESPAD Report and its analyses focused on factors hidden in cultural attitudes such as: the acceptation of exploration and experiments with different drugs during

[28] *Ibidem*.

[29] I. Blatt-Eisengart, D.A. Drabick, K.C. Monahan, L. Steinberg, *Sex differences in the longitudinal relations among family risk factors and childhood externalizing symptoms*, "Developmental Psychology", 2009, no. 45(2), pp. 491–502, https://doi.org/10.1037/a0014942.

[30] I. Grzegorzewska, M. Farnicka, *Attachment and the risk of mental health disorders during adolescence*, "Health Psychology Report", 2016, no. 4(1), pp. 8–15, https://doi.org/10.5114/hpr.2016.54545.

[31] D. Jones, A. Husson , J. Manning, E. Sterrett, *Adolescent Alcohol Use in Context: The Role of Parents and Peers among African American and European American Youth*, "Cultural Diversity and Ethnic Minority Psychology", 2008, no. 14(3), pp. 266–273, https://doi.org/10.1037/1099-9809.14.3.266.

adolescence (high availability, social meetings with alcohol and drugs). Another problem is a big advertising market in cultural space connected with non-abstinence patterns of behavior. The design and delivery of effective evidence-based responses to drug problems is a central focus for European drug policies and involves a range of measures. Prevention and early intervention approaches aim to prevent drug use and related problems, while treatment, including both psychosocial and pharmacological approaches, represents the primary response to dependence. As a summary, four conclusions could be prepared.

1. There are differences between schools, parents and between individuals in how they implement prevention programmes. Even programmes that were designed at the national level or at the European level as intensive programmes can be implemented more or less intensively, depending on the resources and commitment, and family and teachers' attitudes.
2. In all cases, the programmes should be based on real new knowledge, not on stereotypes or expectations based on cultural patterns.
3. Values such as health and being free of dependencies should be taken under consideration and underlined in preparing new programmes. It should be recognized what is hidden in health values in each society.
4. From the general level the patterns of spending leisure time without alcohol or other drugs may be a key to finding a universal solution.

Ethical approval: This article does not contain any studies with human participants or animals performed by any of the authors.

References

1. *Assessment of the added value of the EU strategy to support Member States in reducing alcohol-related harm*, December 2012, https://ec.europa.eu/health/sites/health/files/alcohol/docs/report_assessment_eu_alcohol_strategy_2012_en.pdf
2. Blatt-Eisengart I., Drabick D.A., Monahan K.C., Steinberg L., *Sex differences in the longitudinal relations among family risk factors and childhood externalizing symptoms*, "Developmental Psychology", 2009, no. 45(2), pp. 491–502, https://doi.org/10.1037/a0014942.
3. Boele-Woelki K., *What Family Law for Europe?*, "Rabels Zeitschrift fur auslandisches und internationales Privatrecht" [The Rabel Journal of Comparative and International Private Law], 2018, vol. 82 (1), pp. 1–30.

4. Bronfenbrenner U., *Making Human Beings Human Bioecological Perspectives on Human Development*, Thousand Oaks, CA 2005.
5. *Brussels IIa Regulation 2201/2003*, https://www.peacepalacelibrary.nl/plinklet/?sid=bloginfo&ppn=263129977 (accessed 13.08.2018).
6. European Monitoring Centre for Drugs and Drug Addiction, *European Drug Report*, Luxembourg 2015, http://www.emcdda.europa.eu/edr2015 (accessed 16.08.2018).
7. European Monitoring Centre for Drugs and Drug Addiction, *European Drug Report*, Luxembourg 2016, http://www.emcdda.europa.eu/edr2016_en (accessed 10.07.2018).
8. European Monitoring Centre for Drugs and Drug Addiction, *European Drug Report*, Luxembourg 2017, http://www.emcdda.europa.eu/system/files/publications/4541/TDAT17001ENN.pdf (accessed 10.08.2018).
9. European Monitoring Centre for Drugs and Drug Addiction, *European Drug Report*, Luxembourg 2018, http://www.emcdda.europa.eu/system/files/publications/8585/20181816_TDAT18001ENN_PDF.pdf (accessed 12.08.2018).
10. Farnicka M., Kuźmik M., *Rola Rodziny w systemie resocjalizacji i profilaktyki społecznej w różnych krajach europejskich i pozaeuropejskich*, [in:] *Teoretyczne i praktyczne aspekty funkcjonowania młodzieżowych ośrodków wychowawczych*, G. Miłkowska, E. Magda (eds), Zielona Góra 2016, pp. 47–64.
11. Grant B.F., Dawson D.A., *Age at onset of alcohol use and its association with DSM-IV alcohol abuse and dependence: results from the National Longitudinal Alcohol Epidemiologic Survey*, "Journal of Substance Abuse Treatment", 1997, no. 9, pp. 103–10, https://doi.org/10.1016/s0899-3289(97)90009-2.
12. Grzegorzewska I. *Dorastanie w rodzinach z problemem alkoholowym*, Warszawa 2011.
13. Grzegorzewska I., Farnicka M., *Attachment and the risk of mental health disorders during adolescence*, "Health Psychology Report", 2016, no. 4(1), pp. 8–15, https://doi.org/10.5114/hpr.2016.54545.
14. Gupta N., Smith N., Mette V., *Child Care and Parental Leave in the Nordic Countries: A Model to Aspire to?*, "IZA Discussion Paper", 2006, no. 2014, https://ssrn.com/abstract=890298 (accessed 5.09.2018).
15. Jones D., Husson A., Manning J., Sterrett E., *Adolescent Alcohol Use in Context: The Role of Parents and Peers among African American and European American Youth*, "Cultural Diversity and Ethnic Minority

Psychology", 2008, no. 14(3), pp. 266–273, https://doi.org/10.1037/1099-9809.14.3.266.
16. Kim J.E., Hetherington E.M., Reiss D., *Associations among family relationships, antisocial peers, and adolescents' externalizing behaviors: Gender and family type differences*, "Child Development", 1999, no. 70, pp. 1209–1230, https://doi.org/10.1111/1467-8624.00088.
17. Kusztal J., *Europejskie tendencje w zapobieganiu przestępczości nieletnich*, „Probacja", 2011, no. 4, pp. 33–34.
18. McFadden A.J., Young M., Markham F., *Venue-Level Predictors of Alcohol-Related Violence: An Exploratory Study in Melbourne, Australia*, "International Journal of Mental Health and Addiction", 2015, no. 13, pp. 506–519, https://doi.org/10.1007/s11469-015-9552-3.
19. PARPA, *Kampanie profilaktyczno-edukacyjne*, http://www.parpa.pl/index.php/profilaktyka-system-rekomendacji/kampanie-profilaktyczno-edukacyjne (accessed 5.09.2018).
20. *The European School Survey Project on Alcohol and other Drugs*, 2015, http://www.espad.org/report/home (accessed 16.08.2018).
21. Thornberry T., Freeman-Gallant A., Lizotte A., Krohn M., Smith C., *Linked lives: The Intergenerational Transmission of antisocial behavior*, "Journal of Abnormal Child Psychology", 2003, no. 31, pp.171–189.
22. Thornberry T., Lizotte A., Krohn M., Farnworth M., Jang S., *Deliquent peers, beliefes and delinquent behavior: a longitudinal test of interactional theory*, "Criminology", 1994, no. 32, pp. 47–83, https://doi.org/10.1111/j.1745-9125.1994.tb01146.x.
23. WHO, *Global status report on alcohol and health – 2014*, 2014, https://apps.who.int/iris/bitstream/handle/10665/112736/9789240692763_eng.pdf;jsessionid=48A9543F4F28A8DE11B0342AE3447148?sequence=1 (accessed 10.07.2018).
24. WHO, *World Health Organization Report Substance Abuse*, 2014, http://www.who.int/substance_abuse/publications/global_alcohol_report/msb_gsr_2014_1.pdf?ua=1 (accessed 10.08.2018).
25. Zamparutti T., White O., Sheate W., Baker J., Borsche B., Goldenman G., Hernandez G. *et al.*, *Assessing and strengthening the science and EU environment policy interface*, "European Commission Technical Report", pp. 2012–2059, https://doi.org/10.2779/1028.
26. Zimberg S., *A dual diagnosis typology to improve diagnosis and treatment of dual disorder patients*, "Journal of Psychoactive Drugs", 1999, no. 31(1), pp. 47–51, https://doi.org/10.1080/02791072.1999.10471725.

CITE THIS ARTICLE AS:
M. Farnicka, *Why doesn't prevention work? Drug and alcohol prevention among adolescents in Europe*, [in:] *Security in Central and Eastern Europe: Cyberspace, Police, Prisons, Transport, Addictions, the Media. Proceedings from the Conference XLIV CICA: "Security in Europe" – 12th Security Forum Krakow, 5–7 June 2018, Kraków, Poland*, Krakow 2020, pp. 120–133, https://doi.org/10.24356/proceedings2018/6.

INTERNATIONAL INFORMATION SECURITY IN THE WORLD

**SECURITY IN CENTRAL AND EASTERN EUROPE:
CYBERSPACE, POLICE, PRISONS, TRANSPORT, ADDICTIONS, THE MEDIA**
Proceedings from the Conference
XLIV CICA: "Security in Europe" – 12th Security Forum Krakow
5–7 June 2018, Kraków, Poland
2020 (136–155); https://doi.org/10.24356/proceedings2018/7

The Role of the Media in Multitrack Diplomacy

Rastislav Kazansky*

ABSTRACT

Conflict resolution and prevention is a challenge for diplomacy. The concept of *multitrack diplomacy* addresses this challenge by emphasising the role of the media in peacemaking. The main role of the media – the press, television and the electronic media – in this respect is to inform the public about issues connected with peace and conflict resolution and to involve the public in discussion. This track of *multitrack diplomacy* bases on the assumption that to avoid the increasing engagement in national conflicts, it is necessary to inform the public about the state of affairs in remote corners of the world. The media shape the public opinion and vice versa, the public in democratic countries has, through the media, an opportunity to express their opinions. Exchange of opinions enables the media to evolve and allows the public opinion to have an impact on policymaking. Most

* Assoc. Prof. Dr. Rastislav Kazansky, PhD., MBA, Matej Bel University in Banská Bystrica, Banská Bystrica, Slovakia; correspondence address: Faculty of Political Science and International Relations, Matej Bel University in Banská Bystrica, Kuzmányho 1, 974 01 Banská Bystrica, Slovakia; email: rastislav.kazansky@umb.sk

attempts to bridge the worlds of conflict resolution and the media have so far been conducted by individual peacemakers, e.g. bloggers; however, their initiatives tend to be of local and short-term character, whereas the efforts to use the media for the escalation of conflicts often enjoy support of the authorities of the conflicting sides.

ARTICLE INFO

Article history
Received: 1.10.2018 Accepted: 4.04.2019

Keywords
conflict prevention, conflict resolution, diplomacy, the media, security, multitrack diplomacy

Introduction: the media, the public and policymaking

The influence of the media on politics has been increasingly discussed in the recent decades; among others, by experts in security sciences. Many of them claim that the media have the ability to influence the policymaking (including that on foreign policy); this should be approached with certain skepticism, because it is very difficult to empirically prove this trend. But it is important to realize and define the impact of the media, especially the public media, which do hold some political power in their hands. The relationship between the media and the public is crucial to understand the relationship between the media and politics. The media, in a way, represents the views of the public in the eyes of politicians, while at the same time they have a great power to influence the public. It should be noted at the outset that the real influence of the media on the public opinion, and on the public in general, is difficult to prove empirically (for example, further in this article, the so called CNN effect shall be mentioned) and the results of research initiatives on this topic differ significantly from one another (partly because the public opinion is difficult to measure, as already mentioned). Yet, a general impression that the media influence public opinion is important for the relationship between the media and politics and for the potential impact of the media on political decision-making.

The mass media is undoubtedly a key communication and information channel in modern society. It provides the citizens with access to information about the world beyond their physical reach; it gives a platform for

a wide public debate (no longer limited to face-to-face communication); in general, it is an important component of the public sphere, as Habermas conceived of it. The media serves both the need of the audience (i.e. the public) to be informed and to participate in public debate, and the needs of the political elites and interest groups, to whom it provides the space for addressing the public and expressing their views.[1] The media is, according to this concept, a two-way communication channel.

The power of the media message (and its related potential impact on the public and on policymaking) depends on the type of the media. Print media have the longest tradition, but their power and the reach of publishing companies has been recently declining. In the elite circles of society, one may expect a relatively large influence of elite journals (such as the American *New York Times*) and opinions presented there; however, a significant societal impact should not be attributed to them today. After a short phase of the dominance of the radio in the first half of the 20th century, television has become the dominant medium. Technological progress gradually spread widely and today most people identify television as the main source of information about public affairs.[2]

Whereas a newspaper article may only be accompanied by photographs, a television feature report can be broadcast directly from the place of events, which, from the point of view of audience perception, seems much more credible and has a stronger appeal. An information-based documentary movie gives a recipient a sense of reality and truth, gets them involved in the story and forces them to take a stand on the issue.[3] It is so because "the images carry more influence in shaping attitudes than words".[4] Therefore, in the research studies on the impact of the media on policymaking, the majority of experts focus on television communication (CNN effect theory is, as the name suggests, not an exception).

Although the author of this article has assumed the same direction, it is necessary at this point, to mention the growing role of the Internet, which has not so far been included in most of the research on this subject. Internet

[1] D. McQuail., *Úvod do teorie masové komunikace*, fourth edition, Praha 2009.

[2] B. Bahador, *CNN Effect in action: how the news media pushed the West toward war in Kosovo*, Gordonsville 2007, pp. 5–6.

[3] *Ibidem*.

[4] R. Brown, *Spinning the war: political communications, information operations and public diplomacy in the war on terrorism*, [in:] *War and the media. Reporting conflict 24/7*, D.K. Thussu, D. Freedman (eds), London 2003, pp. 67–90.

news, in the recent couple of years, or better said, decades, have become an increasingly useful source of information on world events. It would be logical to expect its influence on the formation of opinions to grow and to gradually replace the influence of television; however, this trend has not yet been demonstrated. People usually refer to the Internet as a less trusted source, although they admit that they use it.[5] The credibility of the sources in question plays a key role in influencing opinions: it can be assumed that information from the Internet does not make too much influence on people, who would rather choose to seek a second source to confirm it. But one can assume that the various information portals will continue to obtain different degrees of credibility and the influence of the Internet and the new media will gradually grow. Today, it is still too early to involve this phenomenon in the research of such a kind as presented in this work.

1. Multitrack diplomacy[6]

Due to their form, the solving of the current armed conflicts and wars requires new techniques and methods. The activity of multiple non-state actors and the emergence of new forms of violations require the application of new approaches and solutions, which can successfully substitute the traditional forms of conflict resolution. Most importantly, the position of the state in the current international systems is changing.[7]

Multitrack diplomacy (MTD) is a system approach to conflict transformation, which uses a behavioral and organic approach to peacemaking.[8] Within this approach, peace is conceptualized either as a process or as a living organism. MTD eschews the traditional Newtonian mechanistic approach, based on a presumption that the universe and the processes happening in the universe function like a machine which pursues rigorous mathematical rules derived from the action-reaction law. On the contrary, the system approach does not reduce the subject of research into the study of individual units, but it deals with the interconnection of these units and the ways in which they are organized within the system. The number of

[5] B. Bahador, *CNN Effect…*, *op. cit.*

[6] This section is based on the following work: R. Kazanský, *Viacúrovňová diplomacia (multitrack dipolomacy) ako metóda systémového riešenia a prevencie*, [in:] *Súčasné problémy výskumu medzinárodných konfliktov a kríz a ich riešenia*, Banská Bystrica 2013, pp. 173–180.

[7] R. Kucharčík, *Štát v súčasnom medzinárodnom systéme*, [in:] *Aktuálne otázky svetovej ekonomiky a politiky*, Bratislava 2009, pp. 373–379.

[8] J. Galtung, *Peace by peaceful means*, Oslo 1996.

the ties is constantly rising, as does the level of the mutual interdependence between the individual actors of the international political system.[9] The system is characterized not only by its structure and it is not conformed only by the linear law of action-reaction. Systems are growing, developing and transforming. They are analogic to living organisms and characterized by cyclic information flow, non-linear interconnection, and organization characterized by limited autonomy.[10] The specificity of the social system as compared to organic systems lies in the presence of the component of human consciousness in it. Individual parts of the system have the ability to actively and knowingly participate in the organization of the system, while at the same time remaining under the influence of subjective factors. Every individual and every social group is influenced by individual or collective convictions, opinions and values, which influence the human perception of the reality. From this premise a conclusion can be inferred that each conflict is marked by different views of the different parties involved in the same situation.[11] At this point, mass media play a special role.

The term *multitrack diplomacy* is used to indicate a new conceptual approach that reflects the diversity of actors contributing to the peacemaking process in order to build so called positive peace. This concept is basically an extension of so called Track One, Track Two paradigm. The term Track Two was introduced by Joseph Montville from Foreign Service Institute of the US Department of State, who named in this way diplomatic activities situated outside the official governmental activities. Montville made a point that expertise on the conflict necessary to carry out a successful peacemaking process cannot only come from government officials; it has to come from many actors of different origins, with different skills and experience.[12]

Recently, we are witnessing an exponential growth of non-governmental activities in peacemaking processes generally. Track Two, with its content as it was laid out in its original definition, is not able to capture the diversity and complexity of unofficial diplomacy. Later, one of the pioneers of this approach, Louise Diamond, introduced the term *multitrack diplomacy* and John W. McDonald divided Track Two into four tracks: **professional**

[9] B. Kováčik, P. Ondria, *Mierové riešenie konfliktov z hľadiska teórií liberalizmu*, [in:] *Bezpečnostné fórum'09*, Banská Bystrica 2009, pp. 94–101.

[10] M. Duffield, *Global governance and the New Wars*, London and New York 2001.

[11] L. Diamond, J. McDonald, *Multitrack Diplomacy. A system approach to peace*, West Hartford Connecticut 1996.

[12] *Ibidem*.

non-governmental organizations dealing with conflict resolution; **trade**; **private persons**; and **the media**. In 1991, Diamond and McDonald added further four tracks to this model: **religion**; **activists**; **science and education**; and **philanthropy**. Ultimately, the current concept of *multitrack diplomacy* contains nine levels, i.e. **nine Tracks**. Multitrack diplomacy (MTD) is a multidisciplinary approach to conflict resolution with a multi-level system structure. This system is not hierarchized, individual tracks are mutually dependent and interconnected, and therefore the structure is usually shown by means of a pie chart.

Each track has its own resources, values and approaches, and it is a unique and irreplaceable part of the system. All tracks are linked to each other in the center of a diagram and they work on the conflict transformation in mutual synergy. It is a system approach to peace, because not only one part of the system, but all of them together, have the ability of peacebuilding.[13]

Track 1 is the **governmental and diplomatic** level, whose main representatives are governmental and diplomatic representatives of the state, of international and regional organizations, and of international financial institutions such as the IMF or the World Bank. This level represents official diplomacy in the true sense and relates to the classical definition of the state's foreign policies. The actors of Track 1 act on the horizontal level, i.e. they interact with one another, as well as on the vertical level through meetings with local social groups, journalists or university officials. Track 1 is characterized by classical state intervention, which takes such forms as military interventions into conflicts, peacekeeping missions, development aid, or official multilateral and bilateral negotiations. It forms relations of political and bureaucratic character and it is the carrier of the legitimacy of the state power. International official diplomacy is most recently exercised in the United Nations in the form of cooperation and consultations. States and international organizations play the key role in conflict resolution, because their common decisions, but also disagreements, influence the positions of the conflicted parties and the overall development of the conflict.[14] The shortcoming of the official diplomacy is that its analysis often lacks the internal view, and therefore it is often limited to outlining the simplified scheme of the conflict of two sides, disregarding the multiplicity

[13] *Ibidem*.

[14] *Ibidem*.

and diversity of the actors. The representatives of Track 2 level try to fill this gap in conflict analysis.

The representatives of **Track 2** are **professional non-governmental organizations**, which deal with analysis, prevention, and international as well as national conflict resolution. Activities on this level are based on the belief that unofficial diplomacy offers freedom, which would be impossible in the formal environment of official diplomacy. Greater freedom in action enables to explore the causes of the conflict and the human needs behind it. The representatives of non-governmental organizations are not under the spotlight of the media, and therefore have the space to explore the possibilities of non-public methods of reconciling the conflicting parties. The activities of civil diplomats, or simply non-state actors, have three general goals: "1. improving of the communication, understanding and then relation between the groups or nations; 2. relaxation of the tension, fear and anger through the enemy's image humanizing and following assistance in exploring the other party; 3. influencing the opinions and policies of the Track One representatives, namely the formal diplomacy, and building the foundations for official negotiations".[15] Unlike the official diplomacy, their work is long-lasting and they remain in close contact with the population involved in the conflict, providing the necessary conditions for removing psychological barriers and stopping the process of the dehumanization of the enemy. Among the activities carried out within Track 2, there are problem-solving workshops, mediations within the launched peace process, four-eye diplomacy, conferences, education, trainings, confidence building and institutional structure building. Probably the greatest challenge for Track 2 are financial resources. The sponsors of non-governmental organizations are expecting the outcomes in the form of something tangible and measurable. Unfortunately, conflict transformation is a long-lasting open process, whose outcomes are very difficult to measure. It is possible to create the statistics of the victims of the conflict, but it is almost impossible to measure the quality of the relations and changes in the reciprocal approach of the conflicted parties. Obtaining sponsors in such conditions is therefore difficult and it is visible as the unofficial diplomacy within Track Two is showing its credibility and justification to gain more respect of Track One representatives. As examples of Track Two actors, one can mention the following non-governmental organizations: The Institute for Multi-Track Diplomacy

[15] *Ibidem*, p. 2.

founded by Diamond and McDonald; Search for Common Ground under the command of John Marks; or Conflict Resolution Program founded by former US president Jimmy Carter.[16]

Track 3 represents the area of **trade**, which, by means of its potential impacts, can contribute to peacebuilding. The basic goal of private business is, naturally, profit. However, according to Diamond and McDonald, trade has the ability to contribute to peacebuilding activities, because "it is not isolated phenomenon, but the integral part of the social and political life".[17] There is a generally spread belief that trade needs peace to achieve success. Trade can contribute to the building of peaceful social environment, for example by implementing conscious social and environmental policy.[18] Another evidence of the impact of trade is the initiative of the United Nations called Global Compact, established by the former Secretary General Kofi Annan during The World Economic Forum in Davos in 1999. It is a voluntary alliance among UN agencies (UNDP, UNEP, UNHCHR, and ILO) and the representatives of private business sector, whose goal is to humanize international trade activities and to contribute to the development of peace and stability in the world. The alliance has been founded on shared principles such as respect for human rights, working conditions and environmental protection, which should lead to the prevention of the exploitation of cheap labour force.[19] Finally, healthy economy and prosperous trade increase the living standard of the population and decrease poverty, the latter being a triggering factor of black economy and related social phenomena correlated with new wars.

Track 4 relates to **civil diplomacy** and includes unofficial and informal contacts between the members of conflicted communities, who try to influence the public opinion so as to gain human and material sources for the projects that can help in conflict resolution process. Meetings between

[16] *Ibidem*.

[17] *Ibidem*, p. 52.

[18] *Ibidem*.

[19] Global Compact initiative invoked, despite the original selfless intentions, the wave of protests from non-governmental member organizations of the Alliance for a Corporate--Free UN, which believed that the Global Compact would serve transnational companies as a tool for boosting their international image without any concrete commitments. According to the critique, the UN initiative defined its principles too generally and it did not impose any control mechanisms on their observance. Cf. M.L. Maniscalco, *Constructing/Deconstructing the Enemy: A Sociological Perspective*, [in:] G. Aubry, *Sociologia dei processi di pace*, Roma 2006/2007.

interest groups from both warring communities, the organization of concerts and other cultural events, the creation of partnerships between the cities, cultural exchanges, joint research projects, the adoption of children – all these activities are the initiatives of private persons, who, owing to the support of their municipalities, develop better relations between the warring communities. Emphasizing the value of multiculturalism results in removing barriers between communities, in the creation of the relations at the unofficial level, and in so-called empowerment of the self-consciousness of individuals and groups in their ability to contribute to the transformation of conflict environment.[20]

Track 5 refers to **research, training and education**, and it is the intellectual component of the *multitrack diplomacy* system. Its position in the system is legitimized by the belief that the more we know, the more we are able to contribute to the world issues resolution, including the national conflicts. Track 5 is based on the belief that it is important to educate people in order to achieve positive changes, because ignorance breeds mistakes and errors in concrete actions.[21] Track 5, represented by scientists and students in the field of peace and conflict studies, is the "brain" of the systemic approach to conflict transformation, and as such is a creative and innovative source of the free development of theories and approaches. The activities of the actors of Track 5 are various: they analyze the situation, the region or a concrete conflict; they create the syntheses of the evaluated facts and events; they organize seminars and conferences at which the outcomes of the research conducted by various institutions are mutually evaluated; they issue expert publications; they deliver expert comments on the radio and on television, thus influencing the representatives of the official diplomacy as well as the public opinion. Thanks to the activities of its actors, Track 5 is a reliable expert source of information for all other parts of *multitrack diplomacy* system. A downside of Track 5 is that the outcomes of the work of its representatives are considered by them as a goal in itself and not as a tool for other tracks.[22]

The representatives of **Track 6** are interest groups dealing with concrete **social problems** as, for example, respect of human rights or social injustice. Unlike civil diplomacy, which deals with the formation of the mutual

[20] L. Diamond L., J. McDonald, *Multitrack Diplomacy…*, *op. cit.*

[21] *Ibidem*, p. 70.

[22] *Ibidem*.

understanding of warring parties, the actors of Track 6 are reacting by protesting the decisions and actions of the politicians, international organizations and transnational corporations, in order to show their objections as the citizens of the global society, who feel moral responsibility for the world management. The members of these interest groups are also called activists, while their tool are mainly demonstrations activating the wide masses of the population against the immoral behavior of the states and international organizations. Typical examples of the activism of this type are anti-globalists, Amnesty International, Human Rights Watch, Witness for Peace, or Greenpeace. The main significance of the activists in the system of Multitrack Diplomacy is that they are functioning as an alarm signalizing an incorrect procedure of Track 1, while they seek to balance the impact of the official diplomacy. By attracting the attention of the general public, they are a particular controlling administrator who takes care that Track 1 does not abuse its power. Track 6 represents the voice of the people who are not present in the political processes and it contributes to the fairer global governance. The shortcoming of protest movements is that they are a priori defined as anti-systemic, aimed against something. The activities of the protest movements are motivated by anger and rancor, which have the tendency to telescope the activists' attitude instead of sparking dialogue with Track 1.[23]

Religion as a set of spiritual values and principles of behavior is marked as **Track 7**. Religious differences can, in practice, become a source of conflict, but they can also be catalysts for reconciliation. Since religious leaders wield certain authority in their communities, their words have a significant impact on the behavior of individuals and groups. Western religious denominations, in the form of various branches of Christianity, are active in the conflict environment via the communities of believers and church missions, promoting general moral principles such as a charity, compassion and forgiveness. These communities of believers contribute to the same areas of negotiations as other tracks, i.e. the education of the population and local leaders; informal negotiations; mediation; the provision of humanitarian aid; appearance in the media; publishing activity. The contribution of religion to the peacemaking process is that it brings "a spiritual impulse full of idealism of ethical values".[24] In the broader context, one can also

[23] *Ibidem*.

[24] *Ibidem*, p. 101.

positively assess the integrative function of religion as a part of culture. For this integrative function, however, other social institutions are also used, such as educatory units, families, registered partnerships, communication institutions etc. Culture is understood as something positive, which aids convergence and mutual understanding between nations and states; it helps to dull the blades of international contradictions. This idea is only a half-way idea, because the whole problem of culture and religion, and their role in the international environment, is much more complex and internally inconsistent.[25] The negative side of Track 7 is that it has historically had an inclination to exclusivism. It means that a religious community usually only considers its own principles as correct, and it applies these principles to segregate other religious communities.[26]

Track 8 refers to **foundations and individual philanthropists**, whose function in the system is to provide the financial and material sources for the activities performed within other tracks. By the provisioning of financial sources for projects, it determines the agenda and defines the priorities in peacemaking processes. Sponsors and foundations are in the position of a filter that decides which project will enter the system and obtain the opportunity to get visible. In other words, it depends on foundations, which problem or intrastate conflict will be considered as urgent in a given moment and which one will have the opportunity to get visible on the international scene. Some foundations are financed from regular donations, others have to search for sources from individual donors, and therefore they spend much of the time by identifying potential donors and persuading them about the necessity of solving a particular issue. Each foundation has in its agenda a delineated target area. For example, big foundations, such as Ford Foundation, Carnegie, or MacArthur Foundation, support, in the first row, academic and research institutions. Small foundations such as Tides Foundation, Threshold, or Plowshares, have, on the other hand, a tendency to finance practical projects.[27]

The media and public opinion represent **Track 9**, which performs the function of providing information and ensuring communication in the system of Multitrack Diplomacy. The main role of the media in this respect is

[25] D. Hoscheková, *Kultúra v medzinárodnom prostredí a medzinárodná komunikácia*, [in:] *Multikultúrne vzdelávanie pre európske občianstvo*, E. Horská (ed.), Nitra 2009, pp. 132–159.

[26] L. Diamond, J. McDonald, *Multitrack Diplomacy…*, *op. cit.*

[27] *Ibidem*.

to inform, through the press, television and electronic portals, about peace and conflict resolution, and to engage the public in discussions. Along with Track 5, representing research, education[28] and training, Track 9 assumes that in order to properly involve the public in the issues connected with international conflicts, it is necessary to inform them about the status and development of the situation in the far areas of the world. The media, in general, form public opinion and vice versa, the public in democratic countries has the ability to express their opinions on a given issue via liberal mass media. The final result of the free discussion is the impact that the media and public opinion generate on the political decisions of the state officials. The media form a vertical link between the official diplomacy of Track 1 and the community, consisting of the individual participants of Multitrack Diplomacy. The media can be divided – according to the kind of program that they offer – into information media and entertainment media. The problem with the information media run by private companies is the obsession of the companies with ratings and profits, which has a significant influence on the role of the media in conflict transformation. An example of a typical program in the information media is a news show, which often broadcasts exciting, shocking and, of course, violent content. In other words: "not only the peace, but also conflicts and violence create the news".[29] A news material on people living in peace may make a boring program for the media. This is the usual attitude of the media to broadcasting the pictures that legitimize non-violence and peaceful conflict resolution. An interesting secondary product of this steady rule is that after some time, the same intensity of violence does not evoke sensations of the same intensity as it used to; it is no longer considered as news any more. A conflict that lasts for twenty years disappears from the evening news and it occurs again when there are acts of more brutality or a progress in the peacemaking process. Media programmes of informative character can be considered a two-edged sword, which, in the form of the well-known CNN effect, influences the public opinion and, consequently, may influence the political decisions of the state officials and of the international community on getting involved in the peacemaking process to resolve a given intrastate conflict. However, the media can also have the opposite effect; for example, by broadcasting

[28] P. Čajka, P. Terem, L. Rýsová, *Education and Research Infrastructure Development in the Slovak Republic*, [in:] *A new model of socio-economic development of Slovakia*, K. Ivanička (ed.), Bratislava 2012, pp. 266–282.

[29] L. Diamond, J. McDonald, *op. cit.*, p. 124.

pictures from the unsuccessful actions of the international community, they may cause the lifting waves of protests to stop peacekeeping operations. Largely, Track 9 is used in long-lasting intrastate conflicts – for example in Columbia.[30]

2. The role of the CNN Effect

The increasing prominence of the media in the society outlined above, and the continuous expansion of media coverage, brought the theorists of the late 20th century to the consideration of the influence of the media on foreign policy, especially in case of decisions on whether to intervene in a conflict in a foreign country.[31] The first voices pronouncing presumption of foreign policy being media-driven appeared already after the Vietnam War, when first empirical studies of this trend emerged, although results were often very contradictory. The next wave of research on this topic appeared in the early nineties, respectively, after the Gulf War in 1991, which is referred to as the "first war live". The continuous broadcasting of news directly from the scene of conflict, performed by CNN television, has brought a completely new dimension to the role of the media in war. Operation Restore Hope in Somalia in 1992 was another motive for the birth of the theory on the CNN effect. The debate about the involvement of the media in contemporary foreign policy in this regard was prompted by George F. Kennan, in his editorial for The New York Times in September 1993. Kennan called it the Somali operation impulse.[32] His article provoked a debate among experts and policymakers, from which the theory on CNN effect eventually emerged.

According to this theory, media channels that broadcast news on a continuous basis, such as CNN, have an ability to influence foreign policy decisions, and this effect is mainly attributed to them with regard to the issue of humanitarian intervention. Despite the relatively large number of

[30] D. Adašková, *Humanitárna kríza v Kolumbii ako dôsledok bezpečnostnej situácie v regióne*, [in:] *Interpolis'09*, Banská Bystrica 2009, pp. 351–355.

[31] R. Ivančík, V. Jurčák, *Peace operations of international crisis management*, Ostrowiec Świętokrzyski 2013.

[32] G. Kennan, *Somalia, through a glass darkly*, "The New York Times", 30.09.1993, http://www.nytimes.com/1993/09/30/opinion/somalia-through-a-glass-darkly.html?pagewanted=all&src=pm (accessed 5.05.2017).

analyses carried out on this concept, is its fairly precisely defined.[33] Theorists who dealt with this concept included it in many cases considerably different in scope and influence from one another. One of the most important experts that are currently involved in the research on the CNN effect, Piers Robinson, sees it as a "response of both domestic audiences and political elites to the global events that are transmitted via communication technologies in real time".[34] Livingston, who also investigated the phenomenon, defined it as the impact of new real-time transmitting media on diplomacy and foreign policy. Nye and many others consider it as the continuous impact of the flow of information and reporting on public opinion.[35] There is a noticeable disagreement between the analysts in determining who is influenced by the CNN effect. While Livingston mainly sees foreign policy and diplomacy as the subject of its influence, Nye deems public opinion to be the main dependent variable. Robinson combines these approaches and sees the impact on both the policy and the public. In this paper, the author sees the CNN effect as Robinson does, in the broader sense, i.e. as the effect of continuous reporting both on public opinion and on foreign policy.

The CNN effect and its empirical verification over the last twenty years was dealt with by many theorists and their theoretical and methodological approaches differed significantly; it follows that the results of these studies are different, or often even contradictory. Most often, the reader may meet with the content analysis of media communication, or with the research based on the interviews with political actors, or with a combination of both. The most extensive research carried out through interviewing, conducted by a former journalist Nik Gowing, confirmed the existence of the influence of media on political elites, whose representatives admitted in interviews that the media should influence their decisions. This research (as well as other studies of this type) is often challenged as inaccurate, because it does not have a quality methodological basis and policies can be greatly distorted because of the desire of the respondents to ask or retroactively justify some

[33] R. Ivančík, *Teoreticko-metodologický pohľad na bezpečnosť*, "Vojenské reflexie", 2012, vol. 7, no. 1, pp. 38–57.

[34] P. Robinson, *The policy-media interaction model: measuring media power during humanitarian crisis*, "Journal of Peace Research", 2000, 37(5), pp. 613–633, http://www.jstor.org/stable/425283 (accessed 5.05.2017).

[35] J. Nye, *Redefining the National Interest*, "Foreign Affairs", 1999, no. 78 (4), pp. 22–35.

of their actions. Therefore, a more frequent form of research includes the combination of interviews, content analysis and public opinion surveys.[36]

3. CNN effect structure typology

The CNN effect is usually conceived of very broadly, and the evidence for its existence is, therefore, difficult. Thus, the researchers often distinguish multiple types of the CNN effect, each of the types indicating a particular form of media influence on policymakers and the public. Freedman defines three types, namely the classic "CNN effect" (one that leads to intervention), the "bodybags effect" (the pictures of victims leading to the withdrawal of the mission), and the "bullying" effect (the images of great violence and deadly weapons leading to loss of public support).[37] In the author's opinion, the most appropriate systematization of the CNN effect is that presented by Livingston (1997), who defined five types of factors. These five types of the phenomenon need to be discussed in more detail.

3.1 The accelerating effect

The first type of the CNN effect operates primarily on the process of foreign policy (the process of decision-making concerning intervention), rather than on its outputs. Deciding on the steps of foreign policy or diplomatic negotiations is certainly a process that requires time. Continuous media coverage, on the contrary, is characterized by high velocity in the flow of new information. This mismatch, according to theorists,[38] leads to a situation in which the requests for comments from the media, which often involve constant questions on the next steps, pushes the political actors to act swifter and speed up the negotiations. The media often require the interviewees to present their observations on a given topic in prior, so they cannot consult the answer with other party members or study the necessary analysis of events prepared the relevant departments of the Ministry of Foreign Affairs. If the political elite does not present their stance on a given media-covered topic for a long time, in the eyes of the public it may look improper, and the disapproval of the public is not something to be desired. Therefore, the political actors try to react as quickly as possible. Lloyd Cutler, Bill Clinton's

[36] J. Galtung, *Peace…*, *op. cit.*

[37] L. Freedman, *The politics of military intervention within Europe*, [in:] *War and peace: European conflict prevention*, N. Gnesotto (ed.), "Chaillot Papers", 1993, 11, pp. 37–50, http://www.iss.europa.eu/uploads/media/cp011e.pdf (accessed 5.05.2017).

[38] P. Robinson, *The policy-media…*, *op. cit.*

advisor in the White House once said, when the news appears disastrous to foreign affairs, the president and his advisors feel obliged to comment upon it by the time of the evening news. This trend may either lead to the premature expression of politicians' views, or greatly accelerate the process of the negotiations on the issue.

3.2 The agenda-setting effect

The second type of influence is based on the theory of media studies on agenda-setting. As stated above, the media has the ability of being pro-active in the public debate, or, more precisely, of affecting the intensity with which a given problem is discussed. This effect can have an impact on policy. The media has the ability of altering the order of foreign policy priorities in such a way that some of the topics in the news are given more time and better treatment.[39] Influence in this respect may be opposite to the previously described effect – the importance of some topics may be played down due to low media coverage; it is known as the "other side CNN effect".[40] The news media is always trying to obtain new, updated information, which leads to an inability to handle the problem in the long term.

3.3 The impediment effect

Livingston defines two types of media influence which can be an obstacle in achieving already outlined policy objectives (e.g. success in an ongoing military mission). The first type is, again, strongly associated with the emotional attitudes of the spectators to war, when framing highlights the loss of life of innocent civilians, or the deaths of soldiers deployed to missions. These shots can lead to demoralization and loss of home crowd support. The specific political impact of this effect, however, is controversial and varies according to the circumstances. For example, theorists studied this effect in the Somali interventions but the results clearly did not match one another, so it was uncertain if this effect was there or not.

The second type of media influence acting as an obstacle relates primarily to the military and strategic bodies. As Livingston notes, news organizations

[39] Bahador B., *CNN Effect in action: how the news media pushed the West toward war in Kosovo*, Gordonsville 2007.

[40] Školkay A., *Médiá a globalizácia*, Bratislava 2009.

may reveal information that may lead to unnecessary losses of lives, or even the failure of the mission.[41]

3.4 The stimulating (challenging) effect

Livingston's fourth type, also discussed by Bahador, is defined as media pressure on politicians to intervene in a crisis happening in another country (i.e. the pressure to launch a humanitarian intervention). The repeated processing of crisis and emphasizing human suffering turns into "forcing" political leaders to decide about intervention (by changing their policy's goal or the means to achieve it). Bahador claims that this type of the CNN effect is slightly similar to the effect of termination of the mission, but it differs in time. In the first case, the stimulating influence of the media occurs in the initial stage, before the intervention, while in the latter it happens towards the end of the intervention. In the author's view, the incentive effect of Livingston's fourth type of the CNN effect is similar to the agenda-setting effect, which makes it possible to include the fourth type as its subcategory.[42]

3.5 The potential effect

The last type of the CNN effect that researchers distinguish is essentially empirically proven. The potential effect may also operate on the principle of self-fulfilling prophecy. If in the news brutal and very emotional scenes appear and some political leaders or recognized journalist note that "this alters public opinion", it is likely that it will happen. As already mentioned, many people (including policymakers), despite scientific evidence to the contrary, would still believe that the media influenced the public opinion in such a case.

It is obvious that the effect of the media on political decisions does not occur in all cases. In their investigations of the CNN effect, theorists have identified a few different conditions whose presence is necessary to ensure that the CNN effect could occur. One could identify four conditions for a strong role of media in politics (mediapolitik), which are (1) good media infrastructure, (2) large press readership and television audience, (3) political elites trying to use the media to achieve their political objectives, and (4) the willingness of media representatives to change public policy. Robinson

[41] S. Livingston, *Clarifying the CNN Effect: An Examination of Media Effects According to Type of Military Intervention*, Harvard 1997.

[42] Bahador B., *CNN Effect…*, *op. cit.*

enumerates very precisely the conditions of the occurrence of CNN effect in the decision-making process regarding humanitarian interventions. His model of media-politics interaction reveals that the emergence of the CNN effect depends on the presence of (1) emotional framing accompanied by critical evaluation of government policies and (2) political uncertainty. The relevance of the second condition is also confirmed by many other researchers. For example, Shaw points out that loss of confidence in foreign policy after the Cold War gave space for the influence of the media. Kofi Annan warned that if the government has a clear policy, the influence of television is small; however, if the policy is not coherent, the role of the media grows. Robinson, on the basis of his model, shows that if there is political uncertainty at play, the media mainly serves as a tool for gaining public support for government policy – the CNN effect changes its status and becomes the dominant policy.

Conclusion

Many researchers on the relationship between the media and politics come to the conclusion that the positions of the dominant players in policymaking belong to those that use the media to gain public support and achieve their stated objectives. Several theories have been created that deny the existence of the CNN effect and the influence of media on political factors, but most of the research on the topic recognize the influence of the media on public opinion. Theorists suggest that the impression of the influence that the media exerted on the American political and military circles during the Vietnam War led to the increased efforts at later times to "control" the journalists. Interestingly, the Gulf War, which helped to give a rise to the theory of the CNN effect, serves as the most commonly used example of a successfully "controlled" media war. Chomsky and Herman in their theory of *manufacturing consent* argue that the media serve the interests of the current government policy, focusing on the topics that are beneficial for the government, and submitting the information within acceptable limits.

Another approach to the CNN effect, i.e. the neo-Marxist theory, is based on the assertion that the media generally tend to defend the social, political and economic status quo. They become a tool of political marketing, public diplomacy and, in sharper words, propaganda.

Yet another significant theory that denies the CNN effect is the theory of indexing (indexing theory). According to it, the media has a tendency to follow the entire spectrum of views on the political scene. If recognized

elites do not express their disagreement with government policy (even if it is controversial) the media will most likely express it themselves. However, according to the author of this paper, the media is moving in the realm of "legitimate controversy", which determines the extent of the debate within the political elite.

References

1. Adašková D., *Humanitárna kríza v Kolumbii ako dôsledok bezpečnostnej situácie v regióne*, [in:] *Interpolis'09*, Banská Bystrica 2009, pp. 351–355.
2. Bahador B., *CNN Effect in action: how the news media pushed the West toward war in Kosovo*, Gordonsville 2007.
3. Brown R., *Spinning the war: political communications, information operations and public diplomacy in the war on terrorism*, [in:] *War and the media. Reporting conflict 24/7*, D.K. Thussu, D. Freedman (eds), London 2003, pp. 67–90.
4. Čajka P., Terem P., Rýsová L., *Education and Research Infrastructure Development in the Slovak Republic*, [in:] *A new model of socio-economic development of Slovakia*, K. Ivanička (ed.), Bratislava 2012, pp. 266–282.
5. Diamond L., McDonald J., *Multitrack Diplomacy. A system approach to peace*, West Hartford Connecticut 1996.
6. Duffield M., *Global governance and the New Wars*, London and New York 2001.
7. Freedman L., *The politics of military intervention within Europe*, [in:] *War and peace: European conflict prevention*, N. Gnesotto (ed.), "Chaillot Papers", 1993, 11, pp. 37–50, http://www.iss.europa.eu/uploads/media/cp011e.pdf (accessed 5.05.2017).
8. Galtung J., *Peace by peaceful means*, Oslo 1996.
9. Hoscheková D., *Kultúra v medzinárodnom prostredí a medzinárodná komunikácia*, [in:] *Multikultúrne vzdelávanie pre európske občianstvo*, E. Horská (ed.), Nitra 2009, pp. 132–159.
10. Ivančík R., *Teoreticko-metodologický pohľad na bezpečnosť*, "Vojenské reflexie", 2012, vol. 7, no. 1, pp. 38–57.
11. Ivančík R., Jurčák V., *Peace operations of international crisis management*, Ostrowiec Świętokrzyski 2013.
12. Kazanský R., *Viacúrovňová diplomacia (multitrack dipolomacy) ako metóda systémového riešenia a prevencie*, [in:] *Súčasné problémy výskumu medzinárodných konfliktov a kríz a ich riešenia*, Banská Bystrica 2013, pp. 173–180.

13. Kennan G., *Somalia, through the glass darkly*, "The New York Times" 30.09.1993, http://www.nytimes.com/1993/09/30/opinion/somalia-through-a-glass-darkly.html?pagewanted=all&src=pm (accessed 5.05.2017).
14. Kováčik B., Ondria P., *Mierové riešenie konfliktov z hľadiska teórií liberalizmu*, [in:] *Bezpečnostné fórum'09*, Banská Bystrica 2009, pp. 94–101.
15. Kucharčík R., *Štát v súčasnom medzinárodnom systéme*, [in:] *Aktuálne otázky svetovej ekonomiky a politiky*, Bratislava 2009, pp. 373–379.
16. Livingston S., *Clarifying the CNN Effect: An Examination of Media Effects According to Type of Military Intervention*, Harvard 1997.
17. Maniscalco M.L., *Constructing/Deconstructing the Enemy: A Sociological Perspective*, [in:] G. Aubry, *Socilogia dei processi di pace*, Roma 2006/2007.
18. McQuail D., *Úvod do teorie masové komunikace, fourth edition*, Praha 2009.
19. Nye J., *Redefining the National Interest*, "Foreign Affairs", 1999, no. 78 (4), pp. 22–35.
20. Robinson P., *The policy-media interaction model: measuring media power during humanitarian crisis*, "Journal of Peace Research", 2000, 37(5), pp. 613–633, http://www.jstor.org/stable/425283 (accessed 5.05.2017).
21. Školkay A., *Médiá a globalizácia*, Bratislava 2009.

This article is published within the project VEGA 1/0545/17 – Transformation of the security environment: application of the experience of V4 states at the example of Ukraine.

CITE THIS ARTICLE AS:
R. Kazansky, *The role of the media in multitrack diplomacy*, [in:] *Security in Central and Eastern Europe: Cyberspace, Police, Prisons, Transport, Addictions, the Media. Proceedings from the Conference XLIV CICA: "Security in Europe" – 12th Security Forum Krakow, 5–7 June 2018, Kraków, Poland*, Krakow 2020, pp. 136–155, https://doi.org/10.24356/proceedings2018/7.

ISBN 978-83-64035-72-2