PROCEEDINGS

Estonian Academy of Security Sciences

■ NUMBER 16 ■ 2017 ■

FROM RESEARCH TO SECURITY UNION

SRIEE 2017

SECURITY RESEARCH, INNOVATION & EDUCATION EVENT

PROCEEDINGS

Estonian Academy of Security Sciences

XVI

FROM RESEARCH TO SECURITY UNION

SISEKAITSEAKADEEMIA
ESTONIAN ACADEMY OF SECURITY SCIENCES

Tallinn 2017

Submission Contact

Postal address:	*Estonian Academy of Security Sciences*
	Kase 61, 12012 Tallinn
	Estonia
E-mail:	*teadusinfo@sisekaitse.ee*

Publisher:
Sisekaitseakadeemia
Kase 61, 12012 Tallinn
Estonia

Printed by:
Auratrükk

ISSN 1736-8901 (print)
ISSN 2236-6006 (online)

ISBN 978-9985-67-287-7 (print)
ISBN 978-9985-67-288-4 (pdf)

www.sisekaitse.ee

CONTENTS

FOREWORD

Helina Maasing
Editor-in-Chief

It is my pleasure to introduce the fifth issue of the Proceedings of the Estonian Academy of Security Sciences. Having bound the contributions of almost one hundred authors in the past twenty years, the Proceedings has become one of the most recognisable science magazines in the sphere of international security in Estonia and its surrounding countries. The Proceedings of the Estonian Academy of Security Sciences is one of the few annual journals in Estonia which publishes original security-related research papers. The journal is indexed in the EBSCO database.

This special issue of the Proceedings: From Research to Security Union is linked with the Security Research, Innovation & Education Event (SRIEE 2017), which was held on the 14th and 15th of November 2017 in Tallinn. The aim of SRIEE 2017 was to reduce the gap between research and the market, so that innovative solutions can meet the needs of practitioners and other users. This idea is also reflected in the papers collected for this issue of the Proceedings. The journal reflects the broad base of the issues of internal security, from terrorism and radicalisation to fire safety and domestic violence. Also, from this issue you may find innovative projects, which aim to make societies more secure.

SPEECH FOR THE SECURITY RESEARCH EVENT 2017

Julian King
Commissioner for the Security Union

The development of the genuine and effective Security Union in Europe is about supporting Member States in their efforts to respond to the major security concerns that our societies face today. It's about facilitating the fundamental realisation that in our more interconnected and more globalised world – the security of one Member State is the security of all Member States.

Across Europe we are facing threats such as terrorism, cyber-attacks, or man-made or natural disasters that regrettably cause the loss of hundreds of lives. Since these threats are most often of cross-border or transnational in nature, they are addressed more effectively when tackled at a European level.

The EU's effort is focused on fully understanding the nature of these threats, then creating the policies and tools that are needed to tackle them. Security research contributes in a very substantial way to this process – by enabling the development of innovative security solutions.

EU-funded security research has already been delivering exciting results. The projects being presented to you at this event, I believe, attest to that.

However, these high-quality results do not sufficiently feed through into innovative products available on the marketplace for purchase by buyers. This is the key challenge for the years to come that will, rightly, be addressed.

This SRIEE 2017 comes at an important time for EU-funded research. The final Work Programme for Horizon 2020 was adopted three weeks ago. While of course we will need to pay attention to implementing it over the coming three years, the Commission is also now beginning to shape its vision and to prepare its post-2020 framework programme.

Let me highlight what are for me four important issues for the future programme as concerns security research.

First of all, in order to ensure that within the EU the most up-to-date tools are available for security practitioners we need to continue to programme research and foster innovation specifically targeted to their needs. That means we will continue to need a **dedicated European security research programme**.

Of course, this cannot stand in isolation and we need to ensure that we can benefit from synergies with other relevant programmes such as that for defence research.

Secondly, we need a certain **flexibility** especially to allow us to react swiftly to emerging threats.

Thirdly, the future framework programme must contribute to **overcoming the bottlenecks that prevent the uptake of security research onto the market**. Let me identify some of what this could mean in practice:

- It could mean further developing the use of existing instruments such as pre-commercial procurement or public procurement of innovative solutions.

- It should also mean further promoting the direct participation of practitioners in our projects and in supporting the establishment of networks of practitioners that go well beyond the simple exchange of best practices.

- It might mean that the EU needs to develop a better understanding of the needs and constraints of the procurement bodies that purchase equipment for end-users.

- It should mean harnessing the expertise of EU agencies – such as the European Border and Coast Guard – to bridge the gap between research and what is needed by end users in their daily work.

My fourth and final point is about the **level of funding** for a post-2020 security programme. I will certainly make the case within the Commission for a level of funding for security research that is commensurate with the importance of security challenges in the EU. And I

am sure you will similarly be seeking to persuade your interlocutors at national and EU level.

The more that we can show that security research and innovation is succeeding in making a significant contribution to meeting Europe's security challenges, the more likely there will be a positive reaction to calls for increased funding.

Before concluding, I would highlight that in the coming months the European Commission will be consulting the public on what should be the major "missions" under the future research programme that could support the EU, Member States and other partners in addressing global challenges. I invite all of you already to start contributing to this process in your discussions. We need innovative ideas to help shape an EU security research programme that can deliver innovative solutions to tackle the security threats of the future.

THE ECHO OF TERRORISM WITHIN DOMAINS IMPORTANT TO THE DEVELOPMENT OF THE POLICE

Priit Suve, PhD
Estonian Academy of Security Sciences
Professor at Institute of Internal Security;
Tallinn University
Researcher at School of Governance, Law and Society

Keywords: the police, policing, terrorism, management, public administration, criminology, social psychology

ABSTRACT

From the perspective of safety, terrorism can be recognised as one of the most pervasive phenomenon in the contemporary world. However, this article is not about the terrorism. In the age of interdisciplinarity and relationalism, it is widely accepted that to survive, every profession needs knowledge from other domains. Management, public administration, criminology, social psychology, and the police are, amongst others, the academic domains that have essential knowledge for the development of the police. This article tries to answer the question, how is terrorism an important phenomenon in the field of safety, while giving reference to domains mentioned above. The question is important since it paints a picture of the impact of one prominent issue of safety within domains relevant to the police, and in this way refers to directions that should be taken to succeed in managing the police as well as to design (police) education systems. The results indicate that terrorism is a concept that is often not used in the academic domains discussed in this study, and in this manner emphasizes the value of this study and raises the question: how to mitigate the threat of stagnation or backwardness in the police? Further research is needed to recognise what has been said and which spheres require closer attention.

"Comprehension is not the *source* of competence or the *active ingredient* in competence; comprehension is *composed* of competences." (Dennett 2017, p. 149)

INTRODUCTION

The above cited quote from Daniel Dennett refers to an endless list and combinations of competencies that could compose a comprehension of the police in the field of safety. From which domains the police hope to gain knowledge in a contemporary world, and how these domains are attracted by safety topics relevant to the police? These questions are vitally important for the police as a player in a game with continuously changing partners. A steadily changing task environment combined with the dynamic nature of safety pose challenges for the police that should be answered adequately.

In this article there is no question about the definition of the police, it is more productive to think about which domains are important to the police, and how attractive the issue of safety (using the example of terrorism) is to each domain. The latter is important for the police, since knowledge from other disciplines creates standards to which the police can build upon.

The general purpose of this article is to find out and demonstrate how terrorism is represented in domains from which the police obtain knowledge, in order to be a professional player in the field of safety. Concerning the development of the police and policing, the main question posed in this article is: how terrorism as a major topic in the field of safety is represented within domains that are inevitably related to the development of the police and policing? In answer to this question, we have to first look at the academic literature of a particular domain and, second, put these results into the context of the academic literature of police and terrorism.

Although the purpose of articles like this is to strengthen the field of study (see Webster & Watson 2002, p. XIII) - police and policing in this particular case - the piece however is not (yet) a classical literature review article. The nature of this article is more conceptual, but also holds the

notion and preparational ethos for the literature review research(es) of a particular domain.

One way to find adequate domains for this particular research is to look at police science, and ask what is police science anyway? The police science cannot be grasped by some unique or even definite list of disciplines (see e.g. Greene 2006; Bjørgo et al. 2007; Weisburd & Neyroud 2013; Sparrow 2016; Wood et al. 2017), and for this reason we may say that it is multidisciplinary by nature. Indeed, to develop the police and policing knowledge from management and public administration domains are needed; as a member of society and a player in the field of safety - the issue penetrating all layers and fields of society - knowledge from social psychology is vital; and from the point of the police's core mission - dealing with issues of safety (see United Nations General Assembly 1979; Council of Europe 2001) - criminology, the police and policing are the spheres that need to be studied. Naturally, there are more spheres and disciplines (like psychology, the economy, and so forth) that are also important from many perspectives, but from the point of this article the aforesaid were picked as examples (1) for highlighting the multidisciplinary nature of the field of safety and (2) determining the actual possibilities and limits concerning the related domains of the police. On top of this, terrorism (the topic that inspired the article) is also the subject of research.

The police are always influenced by, but also have an impact on, particular trends in safety and terrorism is one of the most visible and influential phenomenon influencing people's lives in the contemporary world, starting from decisions related to traveling (see e.g. Sönmez & Graefe 1998; Kozak, Crotts, & Law 2007), down to policing strategies (see e.g. Murray 2005; Waxman 2008). It makes sense, while terrorism causes strong reactions in countries affected by it, such as the UK, USA, France, Belgium and so forth. Yet, there are countries (like Estonia) that have not experienced terrorism in the ways seen in the countries mentioned previously, but still positioning terrorism as the most significant problem with regard to safety. (Suve 2016)

Since terrorism as a pervasive phenomenon has a significant impact on safety and the police are one of the most important players, the question arises: how the problem of terrorism is represented in domains

from which the police should gain useful knowledge for development? The interdisciplinary nature of the police requires an adequate and up to date input from other domains. With regard to some particular safety issues, almost no studies exist reviewing the position of certain domains. The latter is important as it gives an insight for others into the position of a particular domain on a certain safety issue (like terrorism). The police's passion concerning safety issues is intelligible, but how about other domains?

This review article provides an overview about how the question of terrorism is represented in the academic literature of management, public administration, social psychology, criminology, the police & policing, from 2001 to May 2017. The starting point of the analysis period concerns the terrorist attack on the World Trade Center in the US on September 11th, 2001. Although the sampling and methodology will be described in detail in chapter 2, it is worth noting some general information about the study. The journals chosen for analysis were picked from the Web of Science and Scopus. The general principles of selection were the following: (1) the selection process of journals started from the most influential by impact factor; (2) journals that had an introduction which offered a possibility for valuable knowledge for this research were chosen for closer analysis; (3) articles to which the title and abstract provided information that promised to offer some advantage to the police or policing were listed. In total 30 journals were chosen, 5 from each domain; 182 articles were listed for the further analysis.

To be clear: the idea of this article is not to create a phonebook (Bem 1995, p. 172) but to explicitate the diverse information published on terrorism - the pervasive phenomena - within the scientific research of the domains that aid in developing the police. This article not only offers a valuable and innovative knowledgebase for the police, but also for scholars from the domains selected, it is merely the introduction and preface for further and more profound research.

This article consists of four main parts. In the introduction the problem and purpose of the study were introduced. In the second part, the areas for review and the concept of terrorism as a pervasive problem for safety will be presented; the third part clarifies the methods and sample of this review article, and the fourth part will focus on particular domains as

well creating an image of the field of scientific research related to the topic, it also clarifies some of the limits of the article and formulates ideas for further research.

1. TERRORISM – THE AREAS FOR REVIEW

Why terrorism? There is an enormous amount of literature published about terrorism, and it is not an easy way to grasp the concept. 'There are hundreds of definitions of terrorism in use' (Schmid 2011, p. 39) and 250 of them are collected and presented in 'The Routledge handbook of terrorism research' (Schmid 2011). Since the primary addressee of this article and further studies related, are people interested in the police or policing, the view of terrorism in this article is open and limited only by the abstract threat or direct violence - no reference is given to the roots and location of terrorism in this particular case. In this article, it is enough to admit the violent nature of terrorism on people's perceptions and behavior. To illustrate and specify the latter, an example from Nobelist Daniel Kahnemann is so astonishing that it has to be presented here. Kahneman explains how recent terrorist acts in Israel have affected his behavior during a visit to the country:

"I was driving a rented car, but I was chagrined to discover that my behavior was also affected. I found that I did not like to stop next to a bus at a red light, and I drove away more quickly than usual when the light changed. I was ashamed of myself, because of course I knew better. I knew that the risk was truly negligible, and that any effect at all on my actions would assign an inordinately high "decision weight" to a minuscule probability. In fact, I was more likely to be injured in a driving accident than by stopping near a bus." (Kahneman 2011, pp. 623-634)[1]

This example of safety in a particular country shows that it is the responsibility of the police to find appropriate organisational design and strategies of policing to mitigate the problem. The quote from Kahneman expresses the insidious nature of terrorism and presents vaguely the possible spheres of knowledge that the police and policy makers should

[1] Page numbers from the e-book.

have in dealing with that kind of issues. So, the need for an interdisciplinary knowledge for policing and governance is becoming clearer. However, another important point related to this 'abstract threat' concerns 'appropriateness' in organisational design and strategic actions. Appropriateness should be understood in this article as an adequacy. Due to the pervasive nature of terrorism, it is easy to overreact in many ways. The latter is famously highlighted by Mueller and Stewart: "To the extent that extreme reactions like multitrillion-dollar wars are considered to be a (self-inflicted) part of the cost of the terrorist attack, they do far more damage to the attacked than is accomplished by the terrorists themselves." (Mueller and Stewart 2016, p. 252)

The irrational threat of violence related to the pervasive nature of terrorism is the 'trousseau' that burdens scholars and practitioners of policing, pushing them on a continuous search for a relevant police organisation with an appropriate combination of police strategies. As it was stated above, the purpose of this article is to find out and demonstrate how terrorism is represented in domains from which the police obtain knowledge in order to be a professional player in the field of safety.

This chapter focuses on the phenomena of terrorism as it was represented in scholarly research. Before looking at terrorism from the view of a particular domain, it is useful to get an overview of the topic in general. The widely used way to get an overview of some topic is to run a search in Google Scholar. Looking at the term 'terrorism' within Google Scholar (17th of July 2017), the top 10 most cited sources are presented in Table 1.

It may be surprising that the most cited source concerns couple violence. Even if running a search for 'domestic violence', it would not be the most influential text. Not surprisingly, all these pieces are worth reading for everyone who wishes to get a brief overview of the topic. The texts listed in Table 1 express many different aspects and views of terrorism, but for a better understanding of the topic and the problem of this article, it would be useful to highlight some points from these pieces.

The most cited text (Johnson 1995) and the journal where it was published (Journal of Marriage and the Family) points to the heart of the phenomena of terrorism - there are no limits or defined fields for terrorism, it can appear from wherever. It is not something outlying or abstract - one can

TABLE 1. The results of a search for the term 'terrorism' within Google Scholar - the 10 most cited sources

	Source	Citations
1	Johnson, M. P., 1995. Patriarchal terrorism and common couple violence: Two forms of violence against women. Journal of Marriage and the Family, pp. 283-294.	2168
2	Pape, R., 2005. Dying to win: The strategic logic of suicide terrorism. Random House.	2070
3	Jongman, A. J., 1988. Political terrorism: A new guide to actors, authors, concepts, data bases, theories, and literature. Transaction Publishers.	1771
4	Pape, R. A., 2003. The strategic logic of suicide terrorism. American political science review, 97(03), pp. 343-361.	1500
5	Crenshaw, M., 1981. The causes of terrorism. Comparative politics, 13(4), pp. 379-399.	1275
6	Krueger, A. B., and Malečková, J., 2003. Education, poverty and terrorism: Is there a causal connection? The Journal of Economic Perspectives, 17(4), pp. 119-144.	1213
7	Baudrillard, J., 2003. The spirit of terrorism and other essays. Verso.	1147
8	Dershowitz, A. M., 2002. Why terrorism works: Understanding the threat, responding to the challenge. Yale University Press.	1062
9	Volkan, V. D., 1998. Bloodlines: From ethnic pride to ethnic terrorism. Basic Books.	1001
10	Laqueur, W., 2000. The new terrorism: Fanaticism and the arms of mass destruction. Oxford University Press on Demand.	1000

Source: Google Scholar, 17th of July 2017.

find it in the home. Another fact is that there are a lot of myths related to terrorism that are not true or can be acknowledged as half-truths. A good example of the latter is the myth of terrorism as a religious or - more precisely - mainly Islamic-related phenomena (see e.g. Crenshaw 1981; Pape 2003, 2005). The examples of couple violence (Johnson 1995) or possible ethnic conflicts (Volkan 1998) will also illustrate the point. For every scientific research the position or starting point should always be clarified. A dualist or dialectical view or just Manichaeist (good or evil, lightness or darkness) paradigm are also too simplistic in handling terrorism - there is no single or clear offender, and it is not always clear what could be the causes and effects. Pape's quote (2005, p. 33) illustrates the later: "Before the US-led invasion in March 2003, Iraq had never experienced a suicide terrorist attack in its history".

Within this murky field of terrorism, there is still at least one thing in common - terrorism is always linked with the dilemma of inclusion-exclusion. The latter is the important characteristic for both: the police and policing. Considering the aforesaid and stressing the aggressive nature of terrorism, from the police's and governance' perspective, it is important to recognise one possible side-effect. Unlike in a war situation where the stronger is not always obvious, in the terror case a terrorist is always weaker compared to the state. Despite the more vulnerable position, a terrorist is hard to catch, and horror is hard to prevent. The 'stronger' has pressure to be even stronger. Baudrillard's (2003, p. 32) statement that "liberal globalisation is coming about in precisely the opposite form - a police-state globalisation, a total control, a terror based on 'law-and-order' measures" is pretty frightening, but not unrealistic. The popularity of stop-and-search techniques of policing (see e.g. Reid 2009; Quinton 2011; Bowling and Weber 2011; Coppock and McGovern 2014) is just one obvious example of the latter.

Although not axiomatic it is hard to dispute the pervasive nature of terrorism and the premise to which domains like management, public administration, social psychology, criminology and the police could be interested in the influences of the phenomena on a particular domain. From that position, we move closer to the point of the current study.

2. METHODS

Since the purpose of the article is to find out and demonstrate how terrorism is represented in the diverse domains from which the police get its knowledge, we should first find the databases offering that kind of information. Although the article has a high ambition of representing the phenomena within diverse domains from a particular perspective, the task is challenging in many ways. On the one hand, it should recognise and express the existence and reverberation of terrorism in some (broad) domain; on the other hand, it should also hold the focus on the police's perspective. Such a complex but tightly focused task reduces the methodological possibilities to run the research, while at the same time making it easier to follow the study.

With the purpose to ensure equal quality of the research data, the sources should also be comparable. The latter enables conclusions to be drawn and to compare the significance of terrorism on a particular domain. For these reasons we need databases different from - for example - Google Scholar, the search engine with various possibilities that is widely used for information retrieval, but may have a low quality of data compared to WoS or Scopus. (See Mongeon and Paul-Hus 2016, p. 14; Moed, Bar-Ilan, and Halevi 2016, p. 27)

For more than 40 years (until 2004, when Scopus was launched by the publisher Reed Elsevier (Archambault, Campbell, Gingras, and Larivière 2009, p. 1320)) the leading academic database was the Web of Science[2] (WoS), where more than 12000 academic journals (including open access journals) are indexed and equipped with an impact factor. The latter enables journals to be assessed and compared, and for this reasons, it is expedient to use as a search engine to fulfill the purposes of this article. In some cases - like in this research - the WoS does not contain all the information required. The reason for that is that some particular domains may not have enough journals indexed in the WoS. For this reason, we turn to another extensive and influential academic databases - Scopus[3]. Scopus contains more than 22000 academic journals (including open access journals), and similarly to WoS, it has a citation metric system. It is appropriate to choose sources from WoS and Scopus for the reason that the data (in the sense of quality) is comparable - "the correlations between the measures obtained with both databases [WoS and Scopus] for the number of papers and the number of citations received by countries, as well as for their ranks, are extremely high ($R2 \approx .99$)". (Archambault, Campbell, Gingras, & Larivière 2009) The allegation that "journals covered by Scopus and not covered by WoS tend to have a low citation impact and tend to be more nationally oriented" (Waltman 2016, p. 8) may concern the 'lower' part of the list of journals within Scopus, and for that reason has no impact on this study. However, for this indirect reason the first selection of journals for this study was made from WoS, and a search from Scopus was only used in cases where the WoS

[2] Follow the link to Web of Science: https://login.webofknowledge.com/error/Error?Error=IPError&PathInfo=%2F&RouterURL=https%3A%2F%2Fwww.webofknowledge.com%2F&Domain=.webofknowledge.com&Src=IP&Alias=WOK5

[3] Follow the link to Scopus: https://www.elsevier.com/solutions/scopus/content

did not index enough journals for the requirements of this study (see the Table 2 below).

TABLE 2. The scope of the study within the selected domains

	Web of Science	Scopus
Management	In the category 'Management' 193 sources were listed	The database was not used
Public management	In the category 'Public administration' 47 sources were listed	The database was not used
Social psychology	In the category 'Psychology, social' 62 sources were listed	The database was not used
Criminology	In the category 'Criminology & Penology' 58 sources were listed	The database was not used
The police & policing	Using the keyword search (police, policing), within the category 'Criminology & Penology' 3 sources of the police and policing were listed	12 sources with the keyword 'police' and 4 sources with the keyword 'policing' were found
Terrorism	Using the keyword search (terrorism), from the category 'International relations' 2 sources were listed (Terrorism and political violence; Studies in Conflict & Terrorism); and from the category of 'Criminology' 1 source was listed (Crime Law and Social Change)	With the keyword 'terrorism' 7 sources were found

Source: WoS, Scopus.

The choice from the selected domains (management, public administration, social psychology, criminology, the police & policing, and terrorism) was carried out on the following principles and applied to both databases:

- The first selection was performed by starting from the top of the list of journals (listed by current impact factor) in every domain. Since the WoS and Scopus do not have precise categories for terrorism, the police & policing, the keyword search with terms 'terrorism', 'police', and 'policing' were examined where needed.

- Since the domains and categories in this study did not match 100 percent in the WoS and Scopus, the aim and scope of the sources were the primary indicators in the first selection. For example in the case of 'Crime, Law and Social Change' the description of the journal indicated a particular focus on terrorism, and for this reason it was added to the domain of terrorism in this study (see Table 3 below), although the journal was listed under the category criminology (WoS). In searching within Scopus, the keyword search was used.

- After the first selection, a search with the term 'terrorism' within every journal (except in terrorism-specific journals) was exercised, and eliminated sources with 0 matches.

- Considering the description (aim and scope) of sources from every domain and the results of the keyword search mentioned above, five sources were chosen for the analysis, and each issue of selected journals from 2001 to May 2017 was screened carefully. Every study that had a relevant title and abstract was chosen for further analysis.

TABLE 3. The list of journals and number of articles that have relevant terrorism-related knowledge for the police

Domain / Title of the journal	IF / Scopus	Selected articles	The year of foundation
THE POLICE AND POLICING			
Policing & Society	1,610	10	1990
Police Quarterly	0,800	10	1998
Policing: An International Journal of Police Strategies & Management	0,761	5	1977
Police Practice and Research	Scopus	18	2000
Policing: a Journal of Policy and Practice	Scopus	6	2007
		49	
CRIMINOLOGY			
Crime and Justice	4,941	1	1979
Journal of Research in Crime and Delinquency	2,446	1	1964
The British Journal of Criminology: An International Review of Crime and Society	1,643	5	1960

Domain / Title of the journal	IF / Scopus	Selected articles	The year of foundation
Criminology & Public Policy	0,769	7	2001
The European Journal of Criminology	1,305	1	2004
		15	
MANAGEMENT			
Academy of Management Journal	6,233	2	1958
Journal of Management Studies	4,131	1	1964
Organization Studies	2,798	1	1980
Organization	1,777	2	1994
Journal of Organizational Change Management	0,577	2	1988
		8	
PUBLIC ADMINISTRATION			
Journal of Public Administration Research and Theory	3,893	3	1991
Public Administration Review	2,636	13	1940
Public Administration	1,922	5	1923
Public Management Review	1,872	2	1999
International Public Management Journal	1,233	6	1997
		29	
TERRORISM			
Studies in Conflict & Terrorism	0,589	23	1977
Terrorism and Political Violence	0,933	18	1989
Journal of Policing, Intelligence and Counter Terrorism	Scopus	13	2006
Critical Studies on Terrorism	Scopus	4	2008
Crime, Law and Social Change	0,492	11	19771
		69	
SOCIAL PSYCHOLOGY			
Social Issues and Policy Review	5,714	3	2007
Political Psychology	2,089	4	1979
Journal of Experimental Social Psychology	2,159	1	1966
European Journal of Social Psychology	1,921	3	1971
Basic and Applied Social Psychology	1,818	1	1980
		12	
Total		182	

Sources: WoS, Scopus, and the webpages of a particular journal.

3. THE ANALYSIS AND CONCLUDING REMARKS

"Terrorism, like viruses, is everywhere." (Baudrillard 2003, p. 10) No matter how you define terrorism - is it in terms of war or crime - from the police perspective it is a challenge anyway. At the same time, everyone who aims to deal with terrorism has to set a focus from the ontological as well as epistemological perspective. For example, regarding safety, terrorism can be seen as a hierarchical relationship that may be one particular precondition for couple violence (see e.g. Johnson 1995), or we may take it as a threat that has an impact on democratic institutions (see e.g. Wilkinson 1986; Pape 2005). In any case, it is hard to overcome one's argument about the pervasive nature of terrorism. The latter is a critical aspect for the police in many ways, but from the perspective of this article, it is important to emphasise the position of safety in domains that offer necessary knowledge to the police. There is no definitive list of these domains, and it is probably appropriate to think that all domains of social life have an influence on, and have been affected by safety - the only question is about the degree of impact at a particular moment in time. The police are in a similar situation: it is useless to try to define the ultimate list of domains from which the police has a chance to learn. At the same time, it is hard to specify the most relevant domains for the police, but domains such as management, public administration, social psychology, and criminology can be seen as the basis from which the knowledge for successful policing and adequate organisational design can be acquired. To gain an overview about how a particular safety issue - terrorism in this article - is represented within the academic literature of these domains, police and the matter of safety (terrorism) are the domains that should be added to research.

This article has the ambition to express an actual context of interdisciplinarity for the police from the outside in. The best way to learn something about the meaning of some phenomena is not to study the phenomena from inside, but the opposite - from the outside. For example, if we want to know how a car works, then we should explore the car; but if we want to know what a car is, then we should look at the car in the context of other artifacts. (See e.g. Toomela 2016) This train of thought is important to follow because from the point of that kind of pervasive phenomena like terrorism, we should first understand and

limit what the police is or could be (e.g. in a particular country), and after that look at and design police work. In answer to the question 'what the police could be,' the other domains come into play. And more particularly, from the point of this article, we could say that for the designers of police organistaion it is of vital importance to know, how the particular problem of safety is represented in domains relevant to the police. Concerning the development of the police and policing, the question arises: what should the police do to get knowledge from the domains that are related to the police and policing? As it was posed in the introduction, in answering this question, we have to first look at the academic literature of a particular domain and, second, put these results into the context of the academic literature of the police and terrorism.

The tables 2 and 3 in this article express, to some extent, (1) the general scope of a particular domain, and (2) how the issue of terrorism is represented in it. Considering the journals listed in every category (within the WoS), management is the most comprehensive domain when compared to the other domains used in this article. While public administration, social psychology and criminology have more or less similar scope, police and terrorism are the least reflected domains. The different scope does not necessarily mean lower quality, but in this case, it expresses the differences of impact factors, which refers to various competitive conditions.

The diverse scope and the results related to this (e.g. impact factor, competition, broader but also diverse list of journals) are the first conclusions to highlight. In order to find the information needed, the preparation and time for screening differs from the other domains under discussion. Since there is an enormous amount of literature in the field of management, it would be almost impossible to specify the only "right" source to follow, and this study is a good example of that. Although five journals were picked, it does not necessarily mean that terrorism is not an interesting or fascinating topic for scholars in the field, but it definitely means that terrorism is not one of the top topics in management studies. Nevertheless, the management sciences - have an enormous scope for scientists - continue to make progress in both a theoretical and empirical sense, both of which may yield something of importance for the police. So, for that reason, for the designer,

managers, and scholars of the police, it is a challenge to be on the ball and see the police through the lenses of management theories.

In this study, the domains like terrorism, police & policing and public administration afford some input to the police and policing, and the result may be somehow recognised as true to type. Nevertheless, it is too early to say something about the content and scope of the input, since such analysis remains out of the limits of this study.

To conclude, I will add some additional notes about the limitations of this article and some directions for further research. This article had the ambition to represent the phenomena (terrorism) within diverse academic domains from the perspective that is necessary to develop the police, and at least to some extent, the purpose was realised. Although the number of domains as well as principles of selection and samples of journals may vary, the main point for the police is quite clear: terrorism and the police are not very often used issues within adjacent academic disciplines. Even in domains like criminology or the police, terrorism was a pretty seldom found topic (in a quantitative sense). Concerning the period (2001-2017) the low interest from criminology (15 articles selected), was the most surprising finding. The latter is especially telling compared to public administration (29 articles selected), social psychology (12 articles selected) or even to management (8 articles selected).

Considering the distinct representativeness of terrorism, the police - in order to advance the police and policing - have limited choices: to outsource the knowledge, to focus police education or to combine the two. It is a challenge for the police education system (and police administration) everywhere. Since terrorism - the pervasive phenomenon and critical problem for safety - receives moderate attention from the domains in this study, the threat of stagnation or backwardness of the police is real, and it is necessary to bear it in mind. The latter is one of the messages of this study.

The conclusions of this article raise at least two significant questions for further research. First, from the point of terrorism, the selected articles from each domain should be carefully examined to get profound knowledge about what was said and what is missing. The second, what

other domains could be related to terrorism which should be studied, and what are the other issues of safety that also demand to be examined. Answers to these questions may depend on the level of analysis as well the purposes and are country-dependent, but it is hard to deny the urgency of these for contemporary policing.

Contacts:

Priit Suve
Estonian Academy of Security Sciences
Institute of Internal Security
Kase 61, 12012 Tallinn, Estonia
Phone: +372 502 4585
E-mail: priit.suve@sisekaitse.ee

Tallinn University
School of Governance, Law and Society
Narva mnt 25, 10120 Tallinn, Estonia
E-mail: priit.suve@tlu.ee

REFERENCES AND SOURCES

Archambault, É., Campbell, D., Gingras, Y., and Larivière, V., 2009. Comparing bibliometric statistics obtained from the Web of Science and Scopus. *Journal of the Association for Information Science and Technology*, *60*(7), pp. 1320–1326.

Baudrillard, J., 2003. *The spirit of terrorism and other essays*. Verso.

Bem, D. J., 1995. Writing a review article for Psychological Bulletin. *Psychological Bulletin*, *118*(2), pp. 172-177.

Bjørgo, T., Romero, F. del B., Kwanten, C., Mawby, R., Pagon, M., and Jaschke, H.-G., 2007. Perspectives of police science in Europe : final report.

Bowling, B., and Weber, L., 2011. Stop and search in global context: an overview. *Policing and Society*, *21*(4), pp. 480–488.

Coppock, V., and McGovern, M., 2014. 'Dangerous Minds'? Deconstructing Counter-Terrorism Discourse, Radicalisation and the 'Psychological Vulnerability' of Muslim Children and Young People in Britain. *Children & Society*, *28*(3), pp. 242–256.

Council of Europe., 2001, September 19. Recommendation Rec(2001)10 of the Committee of Ministers to Member States on the European Code of Police Ethics. Retrieved from http://www.refworld.org/docid/43f5c7944.html

Crenshaw, M., 1981. The causes of terrorism. *Comparative Politics*, *13*(4), pp. 379–399.

Dennett, D. C., 2017. *From bacteria to Bach and back: The evolution of minds*. WW Norton & Company.

Greene, J. R., 2006. *Encyclopedia of Police Science: 2-volume set*. Routledge.

Johnson, M. P., 1995. Patriarchal terrorism and common couple violence: Two forms of violence against women. *Journal of Marriage and the Family*, pp. 283–294.

Kahneman, D., 2011. *Thinking, fast and slow*. Macmillan.

Kozak, M., Crotts, J. C., and Law, R., 2007. The impact of the perception of risk on international travellers. *International Journal of Tourism Research*, *9*(4), pp. 233–242.

Moed, H. F., Bar-Ilan, J., and Halevi, G., 2016. A new methodology for comparing Google Scholar and Scopus. *Journal of Informetrics*, *10*(2), pp. 533–551.

Mongeon, P., and Paul-Hus, A., 2016. The journal coverage of Web of Science and Scopus: a comparative analysis. *Scientometrics*, *106*(1), pp. 213–228.

Mueller, J. E., and Stewart, M. G., 2016. *Chasing ghosts: The policing of terrorism*. Oxford University Press.

Murray, J., 2005. Policing terrorism: A threat to community policing or just a shift in priorities? *Police Practice and Research*, *6*(4), pp. 347–361.

Pape, R., 2005. *Dying to win: The strategic logic of suicide terrorism*. Random House.

Pape, R., 2003. The strategic logic of suicide terrorism. *American Political Science Review*, *97*(3), pp. 343–361.

Quinton, P., 2011. The formation of suspicions: police stop and search practices in England and Wales. *Policing and Society*, *21*(4), pp. 357–368.

Reid, K., 2009. Race issues and stop and search: Looking behind the statistics. *The Journal of Criminal Law*, *73*(2), pp. 165–183.

Schmid, A. P., 2011a. The Definition of Terrorism. In *The Routledge handbook of terrorism research*, pp. 39–98. Taylor & Francis.

Schmid, A. P., 2011b. *The Routledge handbook of terrorism research*. Taylor & Francis.

Sönmez, S. F., and Graefe, A. R., 1998. Determining future travel behavior from past travel experience and perceptions of risk and safety. *Journal of Travel Research*, *37*(2), pp. 171–177.

Sparrow, M. K., 2016. *Handcuffed: What Holds Policing Back, and the Keys to Reform*. Washington, D.C: Brookings Institution Press.

Suve, P., 2016a. *Eesti elanike kujutlused turvalisusest ja politseist 1991-2021*. Analüütiline raport. Politsei- ja Piirivalveamet.

Suve, P., 2016b. *Politsei kui institutsiooni arengu mõtestamise kontseptuaalsed probleemid keerustuvas vastastiksõltuvas keskkonnas*. Tallinn: Tallinna Ülikool.

Toomela, A., 2016. *Kultuur, kõne ja Minu Ise*. Eesti Keele Sihtasutus.

Torraco, R. J., 2005. Writing integrative literature reviews: Guidelines and examples. *Human Resource Development Review*, *4*(3), pp. 356–367.

Torraco, R. J., 2016. Writing Integrative Literature Reviews: Using the Past and Present to Explore the Future. *Human Resource Development Review*, *15*(4), pp. 404–428.

United Nations General Assembly., 1979, December 17. Code of Conduct for Law Enforcement Officials. General Assembly resolution 34/169. Retrieved from http://www.ohchr.org/EN/ProfessionalInterest/Pages/LawEnforcementOfficials.aspx

Volkan, V. D., 1998. *Bloodlines: From ethnic pride to ethnic terrorism*. Basic Books.

Waltman, L., 2016. A review of the literature on citation impact indicators. *Journal of Informetrics*, *10*(2), pp. 365–391.

Waxman, M. C., 2008. Police and national security: American local law enforcement and counter-terrorism after 9/11. *Columbia Public Law & Legal Theory Working*, pp. 1-22.

Webster, J., and Watson, R. T., 2002. Analyzing the past to prepare for the future: Writing a literature review. *MIS Quarterly*, pp. xiii–xxiii.

Weisburd, D., and Neyroud, P., 2013. Police science: Toward a new paradigm. *Australasian Policing*, *5*(2), pp. 13-21.

Wilkinson, P., 1986. *Terrorism and the liberal state* (Vol. 2). Macmillan London.

Wood, D., Cockcroft, T., Tong, S., and Bryant, R., 2017. The importance of context and cognitive agency in developing police knowledge: going beyond the police science discourse. *The Police Journal*, pp. 1-16.

TENSOR: RETRIEVAL AND ANALYSIS OF HETEROGENEOUS ONLINE CONTENT FOR TERRORIST ACTIVITY RECOGNITION

Babak Akhgar, PhD
CENTRIC (Centre of Excellence in Terrorism, Resilience, Intelligence and Organised Crime Research), Sheffield Hallam University, UK
Director of CENTRIC, Professor of Informatics

Pierre Bertrand
Thales Group, La Défense, France
Data Scientist

Christina Chalanouli, PhD
KEMEA, Greece
Senior Researcher

Tony Day, BSc
CENTRIC, Sheffield Hallam University, UK
Technical Lead

Helen Gibson, PhD
CENTRIC, Sheffield Hallam University, UK
Lecturer in Computing

Dimitrios Kavallieros
KEMEA, Greece
Senior Researcher

Emmanuel Kermitsis
KEMEA, Greece
Senior Researcher

Ioannis Kompatsiaris, PhD
Information Technologies Institute
Centre for Research and Technology Hellas, Greece
Senior Researcher (Researcher A)

Eva Kyriakou
European Organisation for Security, Belgium
Project and Policy Manager

George Leventakis, PhD
KEMEA, Greece
Senior Advisor and Scientific Coordinator in European Projects

Euthimios Lissaris
KEMEA, Greece
Police Captain

Simon Mille, PhD
Universitat Pompeu Fabra, Spain
Researcher

Dimitrios Myttas
KEMEA, Greece
Senior Researcher

Theodora Tsikrika, PhD
Information Technologies Institute
Centre for Research and Technology Hellas, Greece
Postdoctoral Research Fellow

Stefanos Vrochidis, PhD
Information Technologies Institute
Centre for Research and Technology Hellas, Greece
Senior Researcher

Una Williamson
Police Service of Northern Ireland
Head of International Programmes

Keywords: counterterrorism, data mining, dark web, social media

ABSTRACT

The proliferation of terrorist generated content online is a cause for concern as it goes together with the rise of radicalisation and violent extremism. Law enforcement agencies (LEAs) need powerful platforms to help stem the influence of such content. This article showcases the TENSOR project which focusses on the early detection of online terrorist activities, radicalisation and recruitment. Operating under the H2020 Secure Societies Challenge, TENSOR aims to develop a terrorism intelligence platform for increasing the ability of LEAs to identify, gather and analyse terrorism-related online content. The mechanisms to tackle this challenge by bringing together LEAs, industry, research, and legal experts are presented.

1. INTRODUCTION

For most citizens, the Internet is a valuable resource in day-to-day life, but for criminals and terrorists, it provides opportunities to exploit the Web as a tool where they can communicate with affiliates, coordinate action plans, raise funds and introduce new supporters or recruits into their networks. These activities present a significant risk to the citizens of Europe.

TENSOR is an EU project funded under the Secure Societies pillar of the Horizon 2020 programme and aims to develop a platform offering Law Enforcement Agencies (LEAs) fast and reliable planning and prevention functionalities for the early detection of terrorist activities, radicalisation and recruitment. The project aims to develop solutions to mitigate this risk from terrorism and prevent future attacks or crimes from occurring by analysing potential terrorism-related content resulting from extremists' open communications and activity patterns online. To this end, a unified platform will be developed, which will allow for multidimensional content integration from heterogeneous online resources, with a view to gathering large amounts of Surface, Deep, and Dark Web content, applying automatic analysis and summarisation, and presenting the collected intelligence through intuitive interactive interfaces.

Informed by the requirements of LEAs and the challenges they face, the TENSOR platform will include beyond state-of-the-art techniques for searching, crawling, monitoring and gathering multimodal and multilingual Web content with the aim of expanding LEAs current reach and information sources. The techniques developed in TENSOR aim to improve efficiency, performance and effectiveness in finding and gathering this content. Once the TENSOR platform has successfully acquired content, information extraction techniques will be employed such as entity-extraction, image, video and audio recognition, as well as automatic translation. This will allow for the content to be categorised against a custom-developed taxonomy for terrorist-generated content. Categorisation will provide the basis for the TENSOR platform to perform an automated analysis of the content, employing techniques such as clustering and classification, social network analytics and semantic

reasoning. After the automated analysis has been performed, the platform will automatically select the most relevant content and generate summaries and visualisations to be displayed to the end-user LEAs. This is expected to significantly reduce "information overload" on LEAs and contribute to an increase in efficiency and performance in analysing terrorist-generated content online. To this end, most processes are automated in TENSOR, however end-users will have the option of reviewing these processes and re-configuring the system, making sure that the outputs fit with what is required, should there be a need to do so. Moreover, EU data protection regulations will be taken into account during the design and development of the system. Measures will be taken to ensure that the principles of a) data minimisation, b) data quality, c) data limitation, d) data protection, e) data portability, and f) data breach notifications are built into the system.

By delivering these capabilities, it is expected that TENSOR will positively impact upon: a) more efficient and effective prevention of terrorist activities organised and planned online; b) faster detection of novel terrorism and radicalisation trends, terrorist-published content and grassroots terrorist cells; c) reduction of "information overload" on LEAs, by automatically summarising and visualising only the relevant content; d) built-in privacy and data protection; e) industry's understanding of LEA requirements, and therefore a positive impact on the development of future products and Europe's overall industry competitiveness.

This article showcases the TENSOR project by presenting the challenges LEAs face and the methodology applied in TENSOR for extracting their requirements (Section 2), the tools and technologies currently being developed as part of the integrated TENSOR platform which aim to advance the state-of-the-art in acquiring, analysing, summarising and visualising terrorism-related Web content (Section 3), a legal and ethical assessment of the current operational environment in several European countries (Section 4), and the impact TENSOR may have on this domain (Section 5), before concluding (Section 6).

2. TENSOR USE CASES: CHALLENGES, METHODOLOGY, AND USER REQUIREMENTS

TENSOR employs an agile user-centred methodology to inform the development of the platform. This includes close consultation with a number of LEAs and security organisations (such as the Police Service of Northern Ireland (UK), Mossos d'Esquadra (Catalonia), National Crime Agency (UK), West Yorkshire Police (UK), Belgian Federal Police, as well as organisations from Greece and Germany) to develop a comprehensive set of requirements for the platform.

These user requirements were created based on specific use case scenarios in four areas pertinent to terrorism: domestic terrorism, international terrorism, lone actor terrorism and radicalisation, and are based on real life events encountered by the LEA partners in the project. Through these scenarios, it was possible to extract and analyse the challenges of LEAs and define the capabilities needed to effectively overcome these challenges. The user requirements were subsequently distilled from the scenarios in the form of Agile User Stories and were gathered first at a high and then at a detailed level. Analysing each high-level requirement into a subset of lower level requirements led to the identification of corresponding functional and non-functional requirements.

Next, we first describe the challenges faced by LEAs while fighting terrorism on the World Wide Web and then depict the use cases/user-requirements.

2.1 CHALLENGES

Through the four use cases and preliminary requirements gathering, the project was able to recognise a number of key challenges that are particularly significant in the terrorism domain and that the TENSOR platform would need to tackle in order to provide functionality beyond that the LEAs already have access to. This section describes those challenges in the context of what information would be required and how such information may currently be used by terrorists; this is classified into the following major categories:

- **Utilising the Surface, Deep, and Dark Web as tools for coordinating, recruiting, training and planning of terrorist acts**: Terrorist groups (and their supporters) use the Web to recruit and train new members, and organise coordinated attacks. Especially the Deep and Dark Web can provide, due to their anonymous and encrypted structure, a safe environment for coordinating and planning attacks, minimising the chances of detection and arrest. They are also used for training and radicalisation by facilitating the sharing and dissemination of information and knowledge (e.g., hacking instructions, calls to actions, propaganda) to less experienced supporters without revealing the publisher's identity or location. Moreover, Hidden Service Marketplaces (HSMs) that exist on the Dark Web, particularly in TOR and the IP2 may remain unknown to LEAs for some time. The automated monitoring of such websites, marketplaces, forums, and social media, using word/video/image recognition software, will enable LEAs to search and scrape online data in a timely manner.
- **Accessing social networks and closed groups:** Gaining access, monitoring, acquiring evidence, and investigating "closed groups" on social networks and closed forums can be challenging. Investigators must often wait several weeks before requesting access to their administrators, as time is needed for accounts to seem authentic and to develop a realistic backstory. Amplifying individual weak-signals of online activities by grouping them together with other behavioural and contextual factors, of the same and/or other persons, can provide a comprehensive picture allowing authorities to assess the level of a potential threat to society. The need to engage in covert Web investigation to elaborate on their suspicions and build a body of evidence requires LEAs to invest in operation time which may not produce concrete results, but only further circumstantial evidence. Thus, an automated process that is able to predict, exploit, and respond authentically to common interaction requests on social media and Dark Web forums could free up investigators' time and gain access to these closed groups, before being taken over by analysts once specific information is required.
- **Extraction and analysis of multilingual multimedia content:** The Web is not simply text-based, but is composed of multiple different content types (including images, video, and audio) published and posted in different languages, utilising different colloquialisms and

idioms (e.g., arabizi). For standardisation, any extracted content needs to be accurately transcribed, translated, analysed, and categorised into languages preferred by the end users of the TENSOR platform so as to be "interpreted" correctly, and in a timely manner, to assist LEA experts in determining their appropriate Course of Action (CoA).

- **Understanding and identifying terrorists' perspectives:** To prevent terrorism and to successfully tackle the underlying causes of radicalisation, LEAs are required to gain a greater understanding at an early stage of the psychological preparations and perspectives of violent extremists, their religious and ideological beliefs and the consequential societal influences. These beliefs form the cornerstone for the claims and desire to fight for religious causes, as well as providing the foundations for developing extremist and fanatic attitudes, their subsequent aspirations to convert unbelievers, and their drive to advance their efforts toward their perceived moral betterment of society and social values, such as social justice, solidarity and freedom.

2.2 USER REQUIREMENTS DEVELOPMENT

The requirements were developed based on the identification of user groups and user stories. Two likely user groups of the TENSOR platform, as determined by TENSOR partner LEAs, are intelligence officers and operational intelligence analysts. These user groups were assigned to a number of user stories based on what their operational activities would be. Each user story forms part of a greater whole known as an "epic" which encapsulates a larger use case. Furthermore, the stories were also assigned to three categories: ingestion, analysis, and storage. These attributes were combined with the LEAs' requirements of the TENSOR platform. These correlations allow each user story to address a single requirement, assisting the technical partners to understand the outcome described and the situation that this requirement will resolve, as the following figure depicts.

FIGURE 1: AGILE USER STORY EXAMPLE

#	Type	Category	As an...<Actor>	I can...<Activity>	So that...<Effect>
01	Epic	Analysis	Operational Intelligence Analyst	Determine whether my suspect is already known to authorities as a person of interest or involved in known terrorist/ organised crime groups or online communities	I know as much as possible about my suspect and their history
02	Story	Ingestion	Operational Intelligence Analyst	Ingest a list of persons of interest into the TENSOR platform	The platform knows the persons of interest that I am interested in

Next, the tools and technologies being developed in TENSOR for satisfying the distilled user requirements are presented.

3. TOOLS AND TECHNOLOGY IN TENSOR

The TENSOR platform is composed of a number of components which will be integrated into a unified platform (see Section 3.4). These components include the methods for identification and extraction of online terrorist content (Section 3.1), the analysis of this extracted (textual and multimodal) content (Section 3.2), and the summarisation, presentation, and visualisation of the analysed content for consumption by LEAs (Section 3.3).

3.1 TERRORIST-GENERATED CONTENT ACQUISITION, PROCESSING AND INDEXING

The discovery and acquisition of online terrorist-generated content is the foundation of the TENSOR platform and all other components depend on the provision of this content. We consider online terrorist-generated and terrorism-related content to correspond to textual and multimedia information available on the Surface, the Deep and Dark Web.

3.1.1 TENSOR Data Models and Sources

Each individual piece of content is referred to as an *artefact*. Examples of artefacts may include, among other things, documents, articles, videos, blog posts, comments and likes. Each artefact may possess many *attributes*, some that are selected and extracted from within the original meta-data and others that are attached to the artefact throughout the various stages of processing. Attributes describe various aspects of the artefact, such as when and from where it was obtained, its unique identity, and may well reference other artefacts.

Entities are extracted from the actual content of the artefact and represent the *things* within the content, e.g., organisations, locations, objects, etc. TENSOR is currently developing a comprehensive taxonomy and ontology of terrorism-related entities and classes, as well as the indicators

required for extracting them from acquired artefacts. There are specific components being developed which will extract entities from both textual and multimedia content in various supported natural languages and dialects. Such extraction gives TENSOR components their mechanism for understanding and reasoning against terrorism-related content.

Artefacts and their entities will be *linked* together, allowing for a graph-based model to form. It is these links that allow patterns in the data to emerge through the various processing mechanisms that will be built into the TENSOR processing pipeline.

Acquiring artefacts, entities and links will take place through the various types of sources available, both open public and restricted. These sources may be grouped into four distinct tiers when considering both the nature of availability and content privacy; these tiers are:

1. **Tier 1: Open public non-personal data**, including all widely available published content such as traditional news media sources, widely recognised blogs, web feeds (i.e., RSS) and public social media streams from organisational groups. This tier of content can, but most often does not contain sensitive or personal data, and is usually matter of fact information.
2. **Tier 2: Open restricted non-personal data**, including generally publically available Web forums and social media groups, which although often involves data created by potentially identifiable individuals, is often topical information and not personal in nature.
3. **Tier 3: Open public personal data**, including public facing social media profiles and posts which although are often publicly available, the author has not necessarily explicitly intended the content to be made public. This also covers information that is more likely to contain personal discussions, such as social media users sending publicly visible messages or comments to each other.
4. **Tier 4: Open restricted personal data**, including anything that requires both authenticated access and an *insider* profile or avatar that is in some way connected to an individual or group in order to monitor or acquire their data. This is the most invasive tier of content acquisition and should only be used in specific investigative scenarios where the appropriate authorisation is in place.

Other guidance on these tiers and the levels of authorisation required for them may come from sources such as the UK's National Police Chiefs Council (2015) who define levels of open source investigation and research based on the extent to which they are overt or covert investigations. As TENSOR may operate across the EU, it must be mindful of the differing legislations in different countries (see Section 4).

3.1.2 Content Acquisition, Crawling, and Extraction

Extraction of content from the Surface, Deep, and Dark Web poses a range of challenges for the implementation of the Web crawlers and scrapers that are employed to obtain such content. On the Surface Web, although there exists a greater body of research, many recent reviews (e.g., Weninger, 2016) have noted that extraction methods fail to keep up with current Web trends and the dynamic content that is often served to the user. One recommendation is to make use of headless browsers to ensure the page is fully rendered before extraction while another is to consider the evolving standards that are being brought in by HTML5. Content on the Deep Web is often hidden behind logins and captchas that make automated access more complex. Furche et al. (2013), He (2013), and Zhao et al. (2016) have all recently proposed mechanisms such as adaptions to the XPath extraction method, using reverse link searching to identify Deep Web sites in the first place, or using specific extraction methods for obtaining content from 'entity' based sites.

The Dark Web provides further crawling, mining and extraction challenges as site discovery in the first place is often more complex. Furthermore, many of these sites may be 'invite only' or only appear for limited time periods. Bouchard et al. (2014) have already proposed a system for distinguishing between terrorist and non-terrorist sites on the Dark Web, in particular noting that the phraseology used on the two types of sites differs massively. Chen (2011) offered a number of suggestions for mining the Dark Web, while Zhou et al. (2005) introduced a knowledge management portal for the storage and retrieval of information relating to terrorist groups on the dark web.

Even within these systems for accessing information across the different layers of the Web, there also remains a consideration around how much

autonomy the TENSOR platform should have when accessing this content. Too much autonomy and there is a risk of the system being accused on conducting surveillance, while too little autonomy will not reduce the burden on intelligence analysts' workload and the platform will not be used to its full potential.

3.1.3 Operational Mechanisms

The mechanisms TENSOR aims to use for acquiring content can be broken down into two categories, active and passive. Active content acquisition covers most uses of the TENSOR content acquisition tools. It involves actively making requests against online services for specific types of content via searches and crawling, both of which can leak information to the service about the tool's intentions. Passive acquisition on the other hand attempts to take a more hands-off approach, by exploiting technologies for monitoring purposes. These technologies include RSS feeds, social media streaming sources, newsletter subscriptions and mailing lists. Passive approaches will be employed as much as possible due to their less revealing approach. However, the need for active mechanisms emerges during targeted investigations. Nonetheless the salient point to keep in mind when conducting such research is the mantra of necessary, proportionate and justified (Association of the Chiefs of Police Officers (ACPO), 2013). TENSOR will employ mechanisms to resist the function creep that pervades in many social media based research tools for law enforcement (Trottier, 2013) and the tendency to keep data long beyond its usefulness.

During the retrieval stage, all content that is acquired will be given a unique identity within the TENSOR platform. Secure Hashing Algorithm (SHA) (see Section 3.4.4) will be employed to provide a verifiable identifier for the content to enable the detection of duplicates as well as to protect content from tampering. On top of hashing, Digital Signature Algorithm (DSA) (see Section 3.4.4) will add tamper proofing to the verifiable identifier (or hash) allowing downstream components and subjects to verify the integrity of the content.

In subsequent stages, TENSOR aims to effectively filter and anonymise all acquired textual and multimedia content. Anything not meeting the

minimum required attributes to be considered terrorist-generated or related will be removed immediately upon detection. Further processing will take place in the TENSOR processing pipeline in order to extract entities and links between the discovered and acquired artefacts; some of this extraction and classification will lead to further cyclical searches to discover more relevant content.

TENSOR aims to store and manage all artefacts, entities, and links in a generic and extensible manner. These are the main types of data within the data acquisition process before additional processing takes over. The use of a generic approach enables simplified indexing of content within underlying database technologies. For example, entities can capture various types of classes simultaneously such as locations and categories, which can be indexed together. This does result in fewer, longer indexes, but advantageously provides the capability to deal with entity types that were previously unknown.

3.2 MULTI-MODAL CONTENT ANALYSIS

The analysis and correlation of information extracted from multimodal content aims to ultimately provide LEAs with threat assessment and early warning capabilities, by uncovering the structure underlying the terrorism-related information and data through clustering, classification, community detection and key player identification in social networks, information source quality assessments, multimedia forensics as well as semantic reasoning and enrichment.

3.2.1 Clustering

Clustering aims to group together multimodal objects about similar topics so as to reduce information overload and increase corroboration through aggregation of multiple sources containing the same information. To this end, TENSOR first applies Formal Concept Analysis (FCA) (Ganter & Wille, 1998) using InClose (Andrews, 2011), a deterministic method of deriving a set of hierarchical clusters, each containing a set of instances (multimodal objects) that share a number of common

attributes, such as the terrorism-related entities identified in the TENSOR taxonomy (including people, objects, locations and events), categories, sources, and extracted keywords. The further down the hierarchy one travels, the more specific (more attributes, fewer instances) each cluster becomes. Both instances and attributes can appear in multiple clusters.

Moreover, clustering in TENSOR also relies on methods applied on a graph of the multimodal objects, where nodes usually represent tuples of multiple modalities (e.g. text-image pairs) and links between any two nodes are assigned in an unsupervised or semi-supervised way (Petkos et al., 2017). Community detection on this graph provides densely connected patterns of mutually related objects, resulting in communities of objects that share similar topics. Extracting the correct number of topics is equivalent to the estimation of the correct number of clusters; these are typically not known a priori. To estimate this number, TENSOR relies on multiple realisations of approaches such as DBSCAN*-Martingale (Gialampoukidis et al., 2016b); such methods are robust to noise (i.e. can deal with data not belonging to any topic) and are also able to scale efficiently.

Experiments performed to evaluate the proposed DBSCAN*-Martingale against well-established and parameter-free community detection algorithms were based on four realistic benchmark networks developed by Lancichinetti et al. (2008). The results indicate improvements in the effectiveness of the proposed DBSCAN*-Martingale community detection algorithm in terms of the Normalised Mutual Information (Danon et al., 2005) and RAND (Rand, 1971) metrics. In particular, the most significant differences to the other approaches for both evaluation metrics are observed for the smallest dataset where DBSCAN*-Martingale indicates improvements ranging from 12% to 35% in terms of NMI and from 5.6% to 8.8% in terms of RAND. In the larger datasets, DBSCAN*-Martingale still performs better than all the other approaches, but the differences in the effectiveness are smaller, particularly for the RAND evaluation metric. The second best performing community detection approach is Walktrap (Pons & Latapy, 2006), with the exception of NMI for the smaller datasets, where the Fast Greedy (Clauset et al., 2004) and the Louvain (Blondel et al., 2008) methods perform second best.

3.2.2 Classification

Classification aims to automatically assign the multimodal objects to specific categories, e.g. regarding the level of radicalisation exhibited by a document consisting of multiple modalities (such as a Web page or social media post) using machine learning and deep learning techniques that exploit the rich information from the different modalities (e.g. text and images) and the inter-connections among them. TENSOR first employs Recurrent Neural Networks (RNNs) to build a text-based model that is learnt based on a set of documents annotated with the specific categories of interest. Given a new document, the model projects it into the produced latent vector space and classifies it to an appropriate category. Regarding images, the same methodology is applied with the only difference that the first layer uses Convolutional Neural Networks (CNNs) instead of RNNs. During these two classifications, latent vectors are extracted for representing respectively the two modalities (i.e. texts and images) into similar spaces so as to merge them. Finally, a third model is learnt to perform the classification by fusing together the two modalities; in this last case, the main challenge is to deal with documents without images and thus make the third model adaptive to this missing input. Preliminary experiments indicate promising results for the individual modalities using RNNs and CNNs respectively, while further research is needed for their combination.

3.2.3 Social Network Analysis

Social Network Analysis aims to detect communities of users (e.g., user accounts on forums/social media platforms) engaging in suspicious terrorism-related communications and also identify the most important and influential actors with a key role in the connectivity of the social network and thus the dissemination of information. For instance, Twitter has been extensively used for promoting and spreading terrorism-related propaganda due to its nature that permits the inexpensive communication of multimodal messages (tweets) to users worldwide; to this end, a top-down approach is often used, with a core group of members spreading a terrorist group's messages, which are then re-shared by other affiliated accounts. For both LEAs and the administrators of social media networking platforms, it is of vital significance to prevent terrorist

groups from spreading their propaganda (to the extent possible), by shutting down accounts who are found to play a central role in this information exchange.

To this end, TENSOR employs centrality measures and in particular entropy-based centrality measures, such as the Mapping Entropy (ME) and the Mapping Entropy Betweenness (MEB) (Gialampoukidis et al., 2016a). Intuitively, one may think of a random walker on the network, standing at a node who picks his/her next step with a probability equivalent to the degree centrality (in the case of ME) and equivalent to the betweenness centrality (in the case of MEB) and is summed over all neighbours of a node. These two measures consider the information that is communicated through nodes who act as a hub (bridge), i.e. those with high values of degree (betweenness) centrality between any two members. In particular, the MEB centrality considers the betweenness centrality of a node and also exploits local information from its neighbourhood; hence, high MEB values indicate that a particular node can act as a bridge for disseminating information, even if their degree centrality is low. In parallel to the key-player identification, a community detection algorithm is used to divide the network into groups of users (communities). The top-ranked key-player is used to enrich the retrieved results, which is achieved by searching for the community the key-player belongs to (Gialampoukidis et al., 2017).

The proposed centrality measure was evaluated in a network formed by user mentions in terrorism-related Twitter accounts, which were retrieved using a set of five Arabic keywords related to terrorist propaganda. As ground-truth, account suspension information from Twitter was used, which marks user accounts as suspended, given that the suspension process is applied when an account violates Twitter rules by exhibiting abusive behaviour, including posting content related to violent threats and hate speech. The top-100 user accounts identified as key players were examined to determine whether they are suspended, active or no longer exist (i.e., accounts which have been temporarily or permanently deactivated). The results indicate that the entropy-based centralities ME and MEB are able to retrieve the first suspended user at position 16, while PageRank follows at position 19. Other centrality and popularity measures, such as closeness, eigenvector and number of followers do not find any suspended users in the top-100 positions of their retrieved

users. We observe that the network is very spread with many bridges and a diameter equal to 27, so key players are expected to be positioned in between many pairs of nodes in the network, exploiting also their neighbourhood's high betweenness centrality.

3.2.4 Information Source Quality Assessment

Information source quality assessment employs a multi-dimensional viewpoint to interpret the notion of "quality", e.g. in terms of reliability, credibility, relevance, precision, etc. This is then also coupled with misinformation and disinformation indicators; the former refers to false or incorrect information that is spread intentionally or unintentionally (but without realising in both cases that the information is untrue), whereas the latter refers to intentionally false or misleading information that is spread in a calculated way to deceive target audiences. Both mis- and disinformation correspond in essence to disruptive information that misleads and/or misdirects LEAs during their investigations. To this end, TENSOR explores an axiomatic framework based on a combination of theories modelling uncertainty (such as Dempster-Shafer) and machine learning algorithms.

3.2.5 Multimedia Forensics

Multimedia forensics aims to detect digital manipulations (in particular splicing and copy-move manipulations) on online images. The main challenges pertain to the extensive degradation of online content due to the large number of re-savings (between the originally captured image and the image that is published online) and the excessive computational cost of powerful forensic analysis methods. Given the fact that a number of different approaches have been proposed in the literature, each of which has shown to be successful only under specific assumptions and cases (Zampoglou et al., 2017), the TENSOR toolbox implements a number of complementary approaches that can be applied on demand to multimedia content of interest.

3.2.6 Semantic Reasoning and Enrichment

Finally, *semantic reasoning and enrichment* aims to first semantically represent all pertinent information into a network of interconnected ontologies, capitalising on advanced knowledge representation and intelligent context-based reasoning solutions; information from external sources (such as other terrorism-related datasets) can also be integrated into these ontologies. Semantic reasoning is then used to further enrich this data, by deriving facts from the relations between concepts on an individual and collective level so as to enable the detection of unusual event and activity patterns, whilst recognising novel instances of usual patterns.

3.3 MULTI-MODAL SUMMARISATION

In TENSOR, one of the objectives is to present to the users the gist of potentially relevant material discovered on the Web in terms of a summary in the language of preference of the user, and to facilitate the interactive exploration of this material using visual analytics techniques. The summarisation module is still at an early stage of development: the general architecture has been defined, but not all submodules have been integrated or implemented. In this section, we describe the modules needed in order to produce the summaries and visualise the results.

Nowadays, the most popular summarisation strategy is "extractive", which tends to select entire sentences from the original text source(s), based on some relevance metrics. The most relevant sentences are concatenated into a summary; see, e.g., (Diligenti et al., 2004) for an overview. Although extractive summarisation can be realised with little linguistic analysis and the resulting summaries are always grammatically correct, they often lack coherence. Furthermore, the original and the summary are in the same language.

Opposed to extractive summarisation is abstractive summarisation. Starting from a conceptual representation of the original information obtained by language analysis, abstractive summarisation creates intermediate linguistic or conceptual structures from this representation,

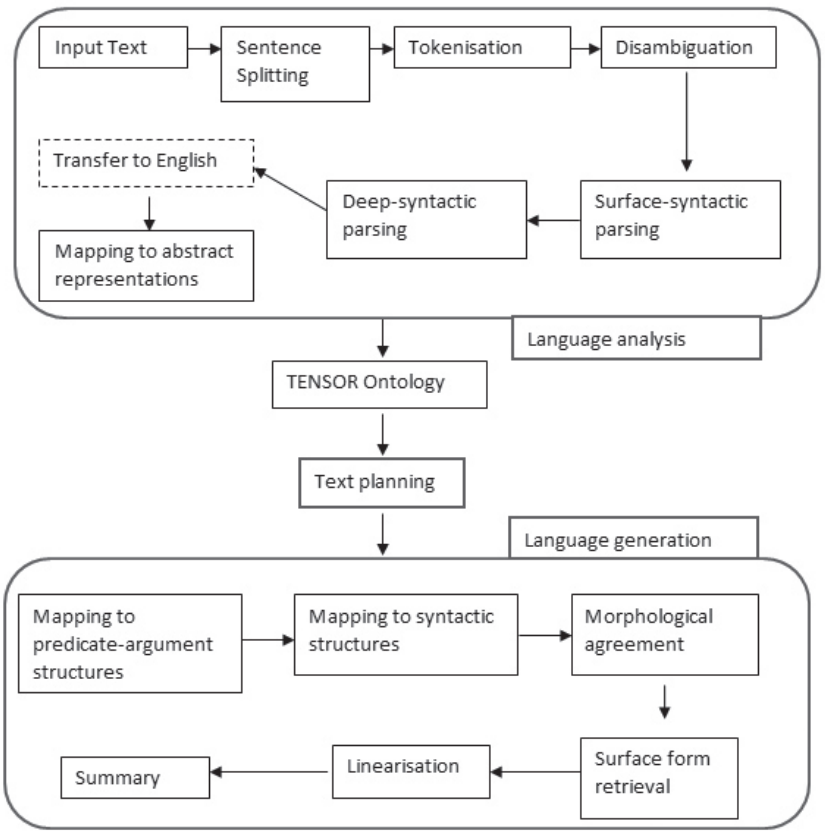
selects the most relevant content chunks and then generates a summary using Natural Language Generation (NLG) techniques. The implementation of our abstractive summariser is based on a sequence of modules that realise the sequence of transitions between different strata. The pipeline can be divided into three main parts:

1. **Language analysis**: Language analysis is carried out by a text analysis pipeline that takes as input the textual content of a document in a given language. This content is first analysed and represented as a forest of abstract syntactic trees. In the case that the input language is different from English, every lexeme in the tree is mapped onto an English lexeme using bilingual dictionaries in order to arrive at a kind of inter-lingua structure that facilitates language neutral representations. These English "inter-lingua" structures are mapped onto semantic structures modelled as RDF triples and then to an ontology.
2. **Text planning**: Conceptual summarisation is approached by assessing the relevance of the semantic structures produced by the language analysis step. Relevance is assessed according to multiple criteria, such as the frequency and joint mention of specific contents in the analysed texts, and lexical-semantic and conceptual relatedness of contents according to lexical databases, sense embeddings and ontologies. Additionally, any inferred knowledge relevant to the domain, the use cases or the production of natural language should also be considered. By considering aspects related to the end user of the system, summaries can be generated tailored to specific users. In addition to determining the relevance of contents, our text planning component also attempts to guarantee a degree of coherence in the summary generated by sorting relevant contents in a sequence that satisfies certain coherence constraints, e.g. grouping together in the text contents that are conceptually related.
3. **Natural language generation**: Following this planning step, linguistic generation starts by transferring the lexemes associated to the semantic structures to the desired target language, using available multilingual lexical resources. Then, the structure of the sentence is determined and all grammatical words are introduced and linked with syntactic relations. Finally, all morphological

agreements between the words are resolved, the words are ordered and punctuation signs are introduced.

In the following, we give more details about the aforementioned modules: language analysis (Sections 3.3.1 to3.3.5), text planning (Section3.3.6), and language generation (Sections 3.3.7 to 3.3.11), as well as visual analytics (Section 3.3.12). Figure 2 shows all the components analysed in the following sections and the connections between them.

FIGURE 2: OVERVIEW OF THE SUMMARISATION PIPELINE



3.3.1 Sentence splitting and tokeniser

Language analysis starts by determining sentence and token boundaries. Rather than addressing tokenisation at a word level, our analysis pipeline treats each sequence of words referring to a specific entity as an atomic unit of meaning. In doing so, we seek to avoid unnecessary internal analysis of multiword expressions which may not even have a strictly compositional meaning (as, e.g., United States of America), and also to eventually obtain predicate-argument structures in which the arguments are not just words, but expressions with an atomic meaning.

3.3.2 Surface-syntactic parsing

In order to determine the syntactic structure of each sentence, we use Bohnet & Nivre's (2012) joint lemmatiser, part of speech tagger, morphology tagger, and dependency parser trained on the CoNLL'09 Penn Treebank dataset (Hajič et al., 2009). This system was the first one to be able to parse non-projective dependency trees while predicting at the same time the part of speech (PoS) and the dependencies, instead of predicting first the PoS and using it for predicting the dependencies in a second step. The authors report an Unlabeled Attachment Score of 93.67, a Labeled Attachment Score of 92.68, and a PoS tagging accuracy of 97.42 (the best possible score being 100 in all cases) in English, improving the state-of-the-art in several languages at the time of publication, and still competitive with current state-of-the-art systems. The sentence splitting, tokenisation and parsing steps require together an average of 65 milliseconds of processing time per sentence.

3.3.3 Deep-syntactic parsing

The objective of this component is to identify and remove all functional words (auxiliaries, determiners, void prepositions and conjunctions) in the surface-syntactic tree and to generalise the syntactic dependencies obtained during the previous stage, while adding sub-categorisation information for lexical predicates. The resulting structures after this step are deep-syntactic trees, in the sense of the Meaning-Text Theory (Mel'čuk, 1988), which is the theoretical framework that underlies the

whole natural language processing pipeline. The mapping between surface and deep syntactic trees can be achieved using rule-based (Mille et al., 2017b) or statistical (Ballesteros et al., 2014) graph-transduction systems. Both systems are able to perform the removal of functional words (*hypernode identification*) with an accuracy of about 99%, and derive the deep dependencies with a recall of about 91% (LAS) in English, for which it is possible to rely on good quality lexical resources (see next section). The deep-syntactic parsing step is currently performed in an average of 25 milliseconds per sentence.

3.3.4 Coreference resolution, word sense disambiguation and entity linking

This step comprises tasks aimed at determining the lexical sense, conceptual meaning or denoted entity of specific words or groups of words in the text. Several state-of-the-art methods and resources for coreference resolution, word sense disambiguation, named entity recognition and entity linking are being considered. Lexical databases and knowledge bases like WordNet (Miller, 1995), PropBank (Kingsbury & Palmer, 2002), VerbNet (Schuler, 2005), FrameNet (Baker et al., 1998), DBPedia (Auer et al., 2007) and BabelNet (Navigli & Ponzetto, 2012) can be used as repositories of senses and entities, possibly extended with domain specific knowledge compiled in collaboration with user partners. For the coreference resolution task, we will experiment with both simple baseline methods, e.g., best mention method based on well-studied syntactic and lexical constraints, and advanced methods such as those implemented in the Standford CoreNLP tools (Manning et al., 2014). Similarly, we will consider a range of methods and tools for the disambiguation and linking tasks, ranging from baselines known to perform well, e.g., most frequent sense, to more complex methods, i.e., those based on features extracted from the local context of mentions of entities, or graph-based global disambiguation methods that aim at producing coherent sets of sense assignments.

3.3.5 Mapping to abstract representations

This component outputs representations that facilitate the mapping to the TENSOR ontologies. For mapping deep-syntactic structures to more abstract linguistic representations, large-scale lexical resources are needed. Unfortunately, such resources are available, at this point, only for English. For this reason, we need to map all input languages to English. Using multilingual resources such as BabelNet, it is possible to obtain the translations of all words into English. Once this is done, the sub-categorisation information in the deep-syntactic structure allows us to obtain Frame annotations on top of connected predicate-argument structures. During this step, shared argumental positions are made explicit and idiosyncratic structuring such as the representation of raising and control verbs is generalised. From the implementation perspective, this task is very similar to that of deep-syntactic parsing, i.e., we are developing graph transducers in order to achieve it. The whole analysis pipeline – from text to abstract representations – has undergone preliminary evaluation in English and obtained Unlabeled Attachment Scores of 74% and 71% for precision and recall respectively (see Mille et al., 2017b), and needs about 150 milliseconds per sentence.

3.3.6 Text planning

Our approach to text planning assumes either a deep linguistic representation with semantic annotations (i.e., disambiguated word senses, links to denoted entities) or a fully conceptual representation based on domain ontologies and upper models if and when it becomes available. As explained before, the main tasks of this module are to assess the relevance of the contents and to structure them in a way that guarantees a coherent presentation in the text. Drawing from the literature in text-to-text summarisation and data-to-text planning, we will experiment with graph-based methods to explore and rank the contents in the semantic repository according to multiple criteria. This method will be supported by recently published resources like semantically annotated corpora and distributional sense embeddings. Additionally, pattern extraction methods will be considered to obtain maximally relevant subsets of contents from the semantic repository, while seeking to ensure that grammatically

and semantically correct clauses and sentences can be generated out of them.

3.3.7 Mapping to output language predicate-argument structures

Starting from the structures provided by the text planning module, first, some idiosyncratic transformations are made to adjust the structures to the predicate-argument format understood by our generation pipeline, and then, the English labels of the nodes are translated into the desired target language using lexicons. These lexicons must not only contain language-specific vocabulary, but also be linked to our pivot language, namely English. Given that BabelNet senses annotated during the analysis stage are language-independent, we will use them as the cross-linguistic link.

3.3.8 Mapping to syntactic structures

Once genuine predicate-argument structures in the target language are available, the first task is to find which node in each structure is most likely to be the root of the dependency tree. That is, we want to identify what will be the main verb of the sentence, or the word that triggers its appearance. Around the main node, the deep-syntacticisation module builds the rest of the syntactic structure of the sentence. In particular, it is able to decide if a main predicate has to be introduced, or what will be realised as an argument, an attribute, or a coordination. The next step in the procedure is to obtain surface-syntactic structures, i.e., to generate all functional words and label the dependencies with language-specific relations, that is, the opposite actions to the ones performed during the deep-syntactic analysis step. As a generator, we also use graph transducers, as described in (Mille et al., 2017a), together with language-specific lexical resources; see, e.g., (Mille & Wanner, 2015). The resulting structure contains all the words that will appear in the final sentence, together with morpho-syntactic features and syntactic dependencies such as *subject*, *object,* etc. that link the words with one another.

3.3.9 Morphological agreement resolution

During the generation of syntactic structures, morphological features of individual words are already inserted (e.g., nominative case for a German subject). During the transition to the morphological structure, agreement is established using the introduced morphological features and the fine-grained syntactic relations in the surface-syntactic structure. For instance, a verb will get its number and person from the element linked to it with the *subject* dependency relation.

3.3.10 Surface form retrieval

The surface forms of the words are retrieved using a full-form dictionary. In order to obtain the full-form dictionary, we will run the morphological tagger of our surface syntactic parser on a large collection of texts and store each possible combination of surface form, lemma and morphological features. We will therefore be able to retrieve a surface form given a lemma and a set of morphological features. The size of the text collection is crucial in order to ensure a large coverage.

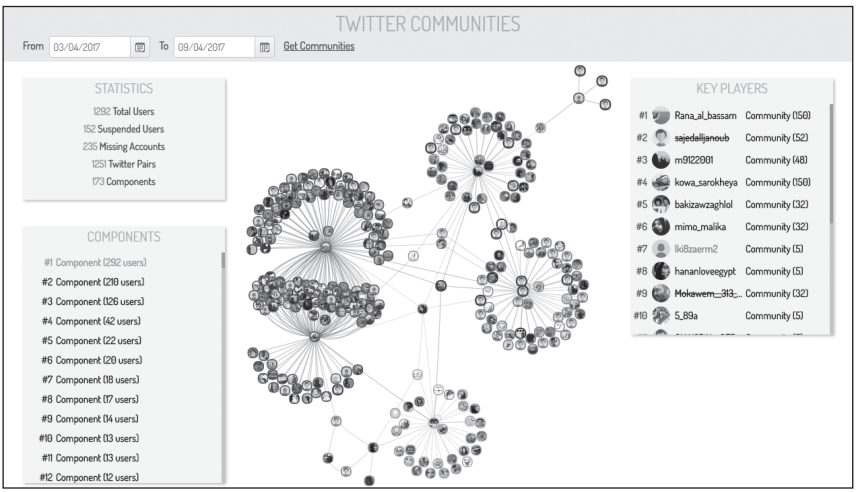
3.3.11 Linearisation

This component takes as input surface-syntactic trees and determines the word order for each tree. In order to ensure large coverage, linearisers will be trained on existing surface-syntactic treebanks, following what has been done in, e.g., (Bohnet et al., 2011), in which the system performs a beam search for optimal word ordering. Words are eventually ordered with a bottom-up method, starting from within subtrees and then ordering subtrees with one another. This linearisation system has obtained high scores on English datasets, with a BLEU score above 89%, and about 58% of the sentences in which all words are ordered exactly as expected.

3.3.12 Visual analytics

Visual analytics algorithms aim to present to the users the analysed and correlated data in a clear and concise interface that allows them to navigate through this information naturally and to improve their situational awareness. For instance, in order to track and flag terrorism-related activities in social media networks, LEAs face big challenges in monitoring relationships and communication activities taking place in such complex networks. To this end, TENSOR proposes a visualisation tool (Andreadis et al., 2017) that offers two novel functionalities based on the key-player identification and key-community detection methods (described in Section 3.2). Both are exposed as a combined Web service and are performed on data from social networks that can be distinguished into statistics, key players and key communities, as demonstrated in Figure 3 for an example from Twitter.

FIGURE 3: SOCIAL NETWORK ANALYTICS VISUALISATION



The network constitutes a straightforward visual representation of how Twitter accounts mention each other and the communities they formulate. Every node in the graph represents a user (profile picture is shown on the node), while every edge is a connection between two users. Communities are indicated by different coloured borders around the

nodes; if an account is inactive, the respective node is coloured red and labelled as "Suspended!" or is coloured black and labelled as "Does not exist!" depending on the case. By clicking on a node, a window pops up to provide more information about the selected user. The pop-up window contains a profile picture on the top left and some account details on the top right, followed by a list of all tweets posted by the featured user. The account details include a name, a username, a description written by the user, a link to the original Twitter page and a label to inform whether the user is suspended or non-existent. Regarding the list of tweets, each item has external links, if any, they are sorted by date and linked to the original tweet. The implementation is based entirely on open-source tools and can be adapted beyond Twitter to instant messaging and other platforms.

3.4 SYSTEM DEVELOPMENT AND IMPLEMENTATION

TENSOR aims to capture, understand and accommodate as many end-user requirements and technical considerations from the earliest stage possible. This section addresses just some of these points by presenting both a high-level overview of the TENSOR architecture and implementation, whilst introducing a small subset of lower-level considerations and challenges where they help elucidate the TENSOR solution.

Developing and implementing a platform such as TENSOR is ambitious and presents many challenges. Although many of these challenges are focussed heavily on the research and delivery of beyond-state-of-the-art tools and technologies aimed to assist LEAs in identifying, monitoring and ultimately combatting terrorism. Behind the scenes there are a myriad of considerations that need to be made to protect the integrity, security, and operation of such tools as well as ensuring straightforward integration and availability. If LEAs are ever going to trust and rely on such technologies, whether independently or within a consolidated platform such as TENSOR, then it is important that under the hood, it is built on an opaque foundation of good pragmatic standards (some of which are introduced in the following sections) and technologies that support the legal and ethical requirements and constraints imposed on LEAs. Furthermore, although TENSOR's output will only be a research

prototype, it is useful to keep in mind some of the proposed security standards required by law enforcement organisations to run an operational product (e.g., PoliceICT, 2017).

3.4.1 TENSOR Architectural Realisation

The TENSOR platform's design loosely follows a Service-Oriented Architecture (SOA) with the main deviation coming from not all components being entirely stateless and the need for a centralised taxonomy and ontology. From a high-level, the system is broken down into many modules or components (defined as services) within three distinctive phases:

1. Discovery and acquisition
2. Analysis and storage
3. Reporting and visualisation

The discovery and acquisition of terrorism-related content will be the source of all data within the system. From here, identified content from a growing collection of *crawl points* will begin its life within the system. It will be given an identity and verifiable hash (see Section 3.4.4) which will uniquely identify each individual piece of content for as long as it is maintained within the system, its archive, or it is deemed irrelevant or unnecessary and is destroyed. This portion of the system consists of several components as discussed earlier in this paper whose responsibility it is to search, crawl, scrape, and interact with various Web- and darknet-based services and sources. The aim is to identify and capture content related to the many aspects of terrorism and terrorist organisations. Once ingested, the data will be passed onto the next phase in order to determine its relevance and validity before it is stored or destroyed.

The analysis and storage phase aims initially to identify for every new piece of content - artefacts and entities - whether it is relevant to the subject of terrorism and whether it is in the interest of both public security and the LEA. TENSOR also aims to capture the key principles of privacy-by-design (Langheinrich, 2001; Cavoukian, 2011) in this phase

to ensure that only data that is absolutely necessary is kept. Any data identified as irrelevant will be immediately destroyed with no further processing, whilst the remainder will be stored in the central content repository. From this point on, select content attributes will be made available on a component-by-component basis for further processing, so that new knowledge and insights can be attained. This higher-level new knowledge will be stored in the central repository and made available to the next phase.

The final phase involves the interaction between the end users and the relevant TENSOR content and knowledge. These components aim to provide the tools for end users to explore and visualise the outputs of the various novel techniques and technologies being developed in TENSOR. Not only that, but they will also have the ability to influence all three phases of the architecture on a case-by-case basis by retrieving and visualising specific sources or types of content and re-configuring the platform's operational focus. This is considered the *value* phase of the system, where the culmination of the TENSOR components and the overall SOA approach provides the end user with insights that they wouldn't have had otherwise.

Across each of these phases will be the growing burden of potentially massive quantities of data that the platform may have to deal with, for which there is little solution other than allocating and managing large storage capacities. For that, clever data management techniques will need to be assessed and implemented. One such issue is the data growth rate, which cannot be mitigated effectively for multimedia given that Web-based multimedia content is often already compressed close to practical limits and although further compression is a possibility, it offers little or no gain. The only real defence is to ensure that multimedia content is not duplicated, achievable by indexing the content hashes (see Section 3.4.4). Textual content on the other hand can be easily, efficiently and effectively compressed automatically via many database technologies.

3.4.2 TENSOR Services Orchestration

For these phases to work effectively, the inter-component communication will be standardised where possible and appropriate. The use of

representational state transfer (REST) interfaces over secure hypertext transfer protocol (HTTPS) connections with JSON and/or XML as the representations of in-transit data appears to have a monopoly in the software industry today. TENSOR makes no aim to deviate from this secure, straight-forward, and trusted approach, but does aim to ensure the best compromises are made between security, complexity and usability are maintained throughout.

At the core of the system will be the central content repository. Not only is this component responsible for managing the storage of all TENSOR content and knowledge, but also the auditing of all activities and interactions with the system. Such auditing is crucial to ensuring the required level of trust and reliability for the use of valuable investigative outcomes in the chain of custody. All of this begins with the fundamental requirement of identity.

3.4.3 Managing Identity

The importance of identity means that every individual piece of content and knowledge created, discovered, stored, or accessed using the TENSOR platform needs to be uniquely identifiable throughout its entire lifetime. TENSOR aims to achieve this using Universally Unique Identifiers (UUIDs) for each and every artefact, entity, and relationship as well as every audited event. Using UUIDs ensures that wherever a piece of data starts its life within the TENSOR platform, it can be allocated an identity without any central coordination whilst confident in the knowledge that the possibility of the same UUID being generated elsewhere in the platform is almost zero.

There are four UUID versions available (Leach et al., 2005), however the expected data growth rates for the platform do not even come close to the operational limitations of properly generated UUIDs, so because of this, they can be chosen based on additional available features and popularity. Version 1 and 4 are the most popular implementations, which can be respectively classified as machine-and-clock based, and securely random. Version 1 is more attractive based on the additional meta-data contained within the UUID. That is a combination of the MAC address of the computer on which it was generated and the time to the nearest

100-nanoseconds, including the central processing unit's (CPU) current clock cycle, making it near impossible to see the same UUID twice over an inconceivable period of time. The additional benefit of version 1 on top of maintaining an audit of the time in which it was generated, is the MAC address which reveals the actual machine that created it. This could be useful for the future verification of the data's original source.

Once all data can be uniquely identified within the platform, it is then possible to log every state change and activity which takes place against each unique piece of data. TENSOR will aim to ensure that this logging is duplicated automatically from the point of creation on both the machine performing the action, in the way of log files, and within the central storage repository in order to ensure multiple sources of the same truth. For every action taking place involving a piece of TENSOR data, its original and unique UUID will be logged with a description of the type of action taking place. Examples of such actions that may be carried out on an artefact or entity include: initial discovery or acquisition; storage; processing; retrieval; visualisation; and removal or archiving.

Each time an action or state change is logged, where there is a process or user responsible, this should also be recorded in order to ensure accountability is always present. TENSOR will aim to ensure that there is no situation where an action can be performed, or the state of the data be changed, where there is no accountable party.

3.4.4 Content Security and Verifiability

Another important and widely used aspect of chain of custody is to ensure the authenticity of the data, primarily to prove that it has not been tampered with in any way since it was originally obtained (Prayudi & Sn, 2015). The current buzz word for LEAs regarding this is "hashing". For example, Interpol already maintains a database of hashed images of child abuse material, which enables the rapid identification of whether a found image is new or not and can help in tracing the source of such images (Interpol, 2017; McCulloch, 2007). A hashing algorithm, as it is known, performs a cryptographic calculation against the underlying data of an artefact, entity, or media file, and generates a relatively short and unique "hash" of the data. The algorithm can easily be re-run at any

point against the subject data and if even 1-bit (or a character in a text file, or a pixel in an image), then the generated hash will be completely different. In fact, this variation in the hashes is what makes them highly reliable. For example, although it may be possible to find or generate two sets of data that would lead to the same hash, it is extremely unlikely that both of these could be valid data of the same type - such as both being images, never mind images that are similar. But, it remains critical that a suitable hashing algorithm, such as the Secure Hashing Algorithm is employed and done so correctly.

TENSOR's aim is to go one step further than hashes alone by investigating the viability and potential additional trust in authenticity gained by combining hashes with the use of Digital Signature Algorithm technology (Kravitz, 1993). Where, for instance, a hash cannot be changed to result in the same media, there is no guarantee that the media hasn't been changed, along with the hash given alongside it. Using DSA would allow the content to be hashed in the same way as before, but to also *sign* the hash with a #verifiable digital signature. It would thus be possible to verify not only that the subject media (or artefact) is authentic, but also that it was actually created by a given component and has not been tampered with.

On the subject of tampering, another important consideration in the development of the TENSOR platform is ensuring the accountability and auditing of activities and that data cannot easily, if at all, be manipulated. Primarily, the project aims to explore write-once read-many (WORM) technologies. These however, can be expensive and require more complex physical hardware and processes to be in place. So, whilst the aim is to investigate and outline recommendations in the use of such technology, softer approaches should also be considered. One way this could be achieved is by implementing tightly secured write-once database restrictions with insert-only privileges and ensuring regular hard backups.

Generally, within the platform, the aim is to mandate effective data security practices across the board, but particularly within the central content repository. Such mandates include, but are not limited to, the use of good standards-based encryption throughout. Primarily this occurs at two obvious points: when data is in transit; and when data is at rest.

Transport Layer Security (TLS) is widely used and heavily standardised. It is also relatively easy to use and configure and should be employed for all inter-component or inter-server communications, even within internal systems. Encryption at rest, on the other hand, deals with any data stored on a physical or virtual storage device, whether live or backup. Again, this is relatively easy to implement and is offered by many database management systems with the use of strong standards-based encryption algorithms. It should be noted that ensuring encryption *keys* are securely managed and all core principles around the chosen standards or algorithms is adhered to is vital for success.

3.4.5 Future Proofing Architecture

Containerisation of software applications, particularly in the micro-services variation of SOA, has been a rapidly growing area of development in the industry. It allows a software application to be wrapped in a standardised container, along with its production configuration and its very own operating system stack - including firewalls. These containers can be rapidly deployed in a standard way and often need only to be plugged together.

TENSOR aims to utilise containerisation, in particular using Docker (https://www.docker.com/), to enable the development teams of each component to configure and deploy how they see fit following black-box principles. As long as each partner respects the agreed inter-component communication protocols, then much of the production-level integration becomes effectively a *plumbing* problem. On top of this, the use of scalable messaging platforms within the platform integration layer is also being considered, which aims to exploit powerful high-availability software principles.

Finally, it is envisaged that TENSOR will not only achieve many exciting and challenging research goals with its many state-of-the-art and beyond-state-of-the-art tools and techniques, but it will also be built in such a way as to enable the highest possible technology readiness and best possible future exploitation opportunities. Much of this will be a result of the project's forward-thinking architectural focus and effective partner cooperation.

4. LEGAL AND ETHICAL ASSESSMENT

The improvement of current regulatory framework is one of the main scopes of TENSOR. A harmonised legal framework is of foremost importance when it comes to the cross-border cooperation of LEAs. In this chapter, we present a general overview of the existing legal procedures in Spain, Greece, Germany and the United Kingdom related to the crime of terrorism.

4.1. SPAIN

In Spain, there are five different public organisations (in three different levels: National, State and Regional) with authorisation to deal with counter terrorism affairs.

The Spanish Criminal Code provides special penal sanctions against terrorism by punishing those who belong to, serve, or collaborate with terrorist organisations or groups (Ministerio de Justicia-Secretaria General Tecnica, 2013). The key approach was the definition of a terrorist organisation or group and the classification of all related illegal behaviours, such as participation in terrorist organisations or groups, and/or simple collaboration with them. Furthermore, the Criminal Code also considers as crimes, individual terrorism and other new types of conduct which impact on the international community, including computer criminal offences.

There are some provisions in the Spanish Criminal Procedure Law (Ministerio de Gracia y Justicia, 2015) regulating the interception of telephone and telematic communications. However, a judicial authorisation has to be issued in order to legally use these investigative methods. The competent Magistrate or the Public Prosecution Services may authorise the Judiciary Police to act under an assumed identity in undercover operations. The undercover agent can only carry out actions necessary to the investigation and proportionate with its purpose. The Spanish Organic Law 15/1999 (BOE-A-1999-23750,1999) intends to guarantee and protect the public liberties and fundamental rights of people regarding the

processing of their personal data. However, this Law and the General Data Protection Regulation are not applicable to the processing of files related to the investigation of terrorism and serious forms of organised crime, or the investigation of other serious criminal offences.

Furthermore, the current Spanish legislation does not provide any reference for the use of search robots in police work. The Criminal Procedure Law introduces provisions concerning the retention of data and other information contained in computers or other electronic devices in order to preserve the integrity and eligibility of these materials in court proceedings.

4.2. GREECE

An electronic investigation should always respect the fundamental human rights stipulated in articles 19 of the Constitution (Hellenic Parliament, 2008) on secrecy of letters and all other forms of free correspondence or communication and 9A of the Constitution for the protection of personal data. However, the Greek legal framework recognises exceptions to the absolute character of these rights for reasons of national security or for the investigation of especially serious crimes, under articles 3 and 4 of Law 2225/1994 (Hellenic Parliament, 1994) on the confidentiality of communications, and article 253A of the Criminal Procedure Code (Hellenic Parliament, 2004) on the investigation of criminal groups. Within this scope, the Hellenic Police can proceed to an undercover investigation, after formal authorisation has been issued by the Prosecutor, or the Prosecutors' Council.

Generally, there are no restrictions on collecting evidence for judicial purposes or police investigations in the case of a serious offence under article 251 of the Criminal Procedure Code (Hellenic Parliament, 2003). The admissibility of automatically generated evidence should also be considered, meaning that as acceptable evidence in court is considered the electronic evidence could be recreated. The Greek legal system stipulates in article 46 paragraph 2 of the Penal Code (Hellenic Parliament, 1951) that whoever intentionally incites others to commit a crime is considered as an agent provocateur. Only the participation in a pre-planned

illegal act, within the framework of an official judicial order could be exonerated.

4.3. GERMANY

In Germany, the term terrorist offence describes every act that aims to seriously intimidate the population or to force or deter public authorities or international organisations from doing something. In addition, terrorist offence describes the act of destabilising or destroying the political, constitutional, economic, or social basic structures of Germany or an international organisation. The lawful interception is regulating the monitoring of telecommunications activities and contents. The legal basis is given by the respective laws such as *§100a of the Criminal Procedure Code (Code of Criminal Procedure*, 2014), the G10 Commission (Basic Law for the Federal Republic of Germany, 2014) and *§23a of the Cu*stoms Investigation Service Act (Germany, 2013). German Intelligence Services as well as LEAs could work undercover to obtain information to prevent and detect crime or disorder and maintain public safety.

In Germany, it is a fundamental right to ensure the confidentiality and the integrity of information technology systems, in order to protect the personal data stored or processed in information technology systems. Infringements of this right are possible within narrow bounds. Preventive state interventions – especially in the framework of online searches – are only permissible constitutionally, if factual indications exist of a concrete danger to a predominantly important legal interest.

The usage of search robots is not mentioned within the German legal framework. However, the collection of special types of personal data is permissible only in so far as inter alia such collection concerns data which the data subject has evidently made public or such collection is necessary in order to avert a substantial threat to public safety. The collection and storage of terrorist content for the purpose of the evaluation of evidence, danger prevention, or the prosecution of a criminal offence is not illegal in Germany. The act of encouraging an individual to commit a crime violates the basic principle of fair proceedings.

4.4. UNITED KINGDOM

First and foremost, terrorism is a crime, which has serious consequences and requires to be distinguished from other types of crime. Individuals who commit terrorism-related offences contrary to UK law are subject to the processes of the Criminal Justice System and those who are otherwise believed to be involved in terrorism are subject to restrictive executive actions.

The British LEAs use all available powers and tactics to prevent and detect crime or disorder and maintain public safety. Undercover policing is one of those tactics. Applied correctly, and supported by appropriate training, it is a proportionate, lawful, and ethical tactic which provides an effective means of obtaining evidence and intelligence, and includes the identification of online terrorist content. The purpose of undercover police officers is to detect or prevent a more serious crime, and to allow an undercover asset to gain the trust of the criminals they are trying to infiltrate. English law offers a defense to someone accused of a crime if they can show an officer acted as an agent provocateur, i.e., they initiated or instigated the crime.

The Data Protection Act 1998 (DPA) (Great Britain, 1998) is the primary piece of UK legislation governing the protection of data. At the heart of the DPA is a set of eight principles, which deal with the collection, use, quality, and security of personal data and with data subjects' rights.

Public authorities can use online research and investigation tools for a specific and legitimate objective – such as preventing or detecting crime, proportionate to the objective in question and in accordance with the law – but they must ensure not to interfere with a person's right to privacy.

The collection of online illegal content by UK LEAs is governed by the Regulation of Investigatory Powers Act 2000 (RIPA) (Great Britain, 2000), regulating the powers of public bodies to carry out surveillance and investigation, and covering the interception of communications. It is an offence to intercept post/public telecommunications within the UK unless authorised under RIPA or another statute (or have consent). A national best practice guide for Digital Evidence has been produced to provide guidance not only to law enforcement, but all stakeholders who assist in investigating cyber security incidents and crime (Williams, 2012).

5. IMPACT

The TENSOR research and designed prototype solutions will have a significant impact on several security operational challenges. The social impact of deploying the TENSOR solution in operational environments will enable LEAs and Security Agencies to increase accuracy towards actionable threat intelligence, make more informed decisions and deliver elevated preventive power. Delivering the platform in the LEAs operational settings will contribute to increased public safety and reduced risk of terrorist activities, whilst protecting fundamental human rights, such as freedom of expression and privacy, thanks to the built-in data protection and anonymisation capabilities of the platform. The early warning of terrorist content or the emergence of networks will allow for early interventions, allowing prevention of radicalisation without criminalisation of subjects.

TENSOR will also contribute to technical and scientific fields. Its innovation activities will improve Web crawling techniques for faster, more efficient content detection and gathering. Research will also focus on effective content gathering from hard to reach silos on the Dark Web and will deliver better information extraction techniques that can deal with larger amounts of multimedia and multilingual content, enable the processing of highly diverse and previously under-utilised online content. Finally, it will improve automated analysis and data mining approaches that help identify relationships between content, the identification of narratives and trends, and the extraction of spatio-temporal patterns of interest.

5.1 IMPACTS ON HOW LEAS FIGHT TERRORISM

TENSOR will provide a unified platform that enables LEAs to effectively detect, categorise, analyse, reason over, and summarise terrorist-generated content. Ultimately, this will increase LEAs capabilities in detecting and preventing terrorist activities organised via the Web, culminating in increased security and resilience across the EU. TENSOR will empower

LEAs to scale their responsiveness and effectiveness through the horizontal diffusion of information. It will also ensure LEAs benefit from a greater range of operational responses thanks to the early identification of terrorist generated content.

The platform will also leverage intelligent mechanisms that identify potential emerging terrorist activities planned and organised via the Internet and make use of enhanced capabilities to support the early detection and identification of online radicalisation.

It is envisaged that the research will also support the deployment of more effective techniques for distinguishing non-harming religious (or other) extremist ideologies from violent radicalisation activities and employ more effective capabilities in gathering data from the Dark Web, which were previously hidden or inaccessible to them. The solutions will also identify patterns as well as uniform responses and prevention measures, which will be undertaken at a strategic level. These impacts are essential to the operational delivery of counter terrorism security in today's ever-changing world.

5.2 ECONOMIC IMPACT

Open Source Intelligence (OSINT) campaigns for law enforcement and counter-terrorism work have become a complex and resource intensive task for both Government and Defence intelligence agencies. OSINT work has gained momentum to become recognised as a legitimate area of intelligence operations, alongside the more traditional intelligence domains such as HUMINT (agent handling) and SIGINT (signals intelligence). This is particularly true in the domain of counter-terrorism. Nearly all Government and Defence intelligence agencies have resources dedicated to the production of OSINT within the intelligence cycle in order to meet their intelligence requirements and to produce actionable outputs.

The security and ICT market segments that are directly addressed by the TENSOR technologies amount globally to approximately 100B USD and one million jobs with conservative estimates. Supporting the

development of TENSOR will result in a highly novel and competitive platform, and an accompanying ecosystem of companies (large ICT providers and SMEs that are part of the consortium, but also companies that are early adopters of the TENSOR technology). This will help European companies that are active in this market segment increase their market share and achieve higher growth rates. Accordingly, we foresee a proportional increase in the number of jobs related to the TENSOR ecosystem (technology development, training, support, sales, etc.). For TENSOR to be able to affect 1% of the pertinent global market will mean to capture 1 billion USD value and to create (or sustain) 10 thousand related jobs. Given the increasing trends of the market and the growing importance of the security sector, TENSOR is on track to deliver a significant and sustainable impact on the European economy.

6. CONCLUSIONS

The internet provides a haven for the creation, sharing, and access to terrorism-related content. It can be a breeding ground for radicalisation and violent extremism, and is one that is largely going unchecked due to the difficulties LEAs have in accessing, analysing and then managing such large amounts of information. The TENSOR platform will, through efficient data capture, text and multimedia processing, analysis and visualisation of such terrorist content, be able to reduce the workload on intelligence analysts and provide operational benefits in the linking of intelligence extracted from such content. TENSOR will serve the operational requirements of LEAs today and in the future by utilising state-of-the-art technologies and algorithms, and by collaborating closely with a number of LEAs that operate on the frontline of Europe's effort to counter the spread of terrorism and violent extremism.

ABBREVIATIONS

CoA: Course of Action
CNNs: Convolutional Neural Networks
CPU: Central processing unit
DPA: Data Protection Act
DSA: Digital Signature Algorithm
FCA: Formal Concept Analysis
HSMs: Hidden Service Marketplaces
HTTPS: Interfaces over secure hypertext transfer protocol
HUMINT: Human Intelligence - Agent handling
IP2: Invisible Internet Project
LEAs: Law Enforcement Agencies
MEB: Mapping Entropy Betweenness
NLG: Natural Language Generation
OSINT: Open Source Intelligence
REST: Representational state transfer
RIPA: Regulation of Investigatory Powers Act
RNNs: Recurrent Neural Networks
SHA: Secure Hashing Algorithm
SIGINT: Signals intelligence
SOA: Service-Oriented Architecture
TLS: Transport Layer Security
TOR: The Onion Router
UUIDs: Universally Unique Identifiers
WORM: Write-once read-many

Contacts:

Babak Akhgar
CENTRIC
Sheffield Hallam University, UK
E-mail: b.akhgar@shu.ac.uk

Pierre Bertrand
Thales Group, La Défense, France
E-mail:
pierre.bertrand@thalesgroup.com

Christina Chalanouli
KEMEA
Leof. Mesogeion 96
Athina 115 27, Greece
E-mail:
c.chalanouli@kemea-research.gr

Tony Day
CENTRIC
Sheffield Hallam University, UK
E-mail: t.day@shu.ac.uk

Helen Gibson
CENTRIC
Sheffield Hallam University, UK
E-mail: h.gibson@shu.ac.uk

Dimitrios Kavallieros
KEMEA
Leof. Mesogeion 96
Athina 115 27, Greece
E-mail:
d.kavallieros@kemea-research.gr

Emmanuel Kermitsis
KEMEA
Leof. Mesogeion 96
Athina 115 27, Greece
E-mail:
m.kermitsis@kemea-research.gr

Ioannis Kompatsiaris
Information Technologies Institute
Centre for Research and Technology Hellas
6th Klm Charilaou-Thermi Rd
Thessaloniki, 57001, Greece
E-mail: ikom@iti.gr

Eva Kyriakou
European Organisation for Security
Rue Montoyer 10, Brussels
Belgium
E-mail:
Eva.kyriakou@eos-eu.com

George Leventakis
KEMEA
Leof. Mesogeion 96
Athina 115 27, Greece
E-mail: gleventakis@kemea.gr

Euthimios Lissaris
KEMEA
Leof. Mesogeion 96
Athina 115 27, Greece
E-mail:
e.lissaris@kemea-research.gr

Simon Mille
Universitat Pompeu Fabra, Spain
E-mail: simon.mille@upf.edu

Dimitrios Myttas
KEMEA
Leof. Mesogeion 96
Athina 115 27, Greece
E-mail:
d.myttas@kemea-research.gr

Theodora Tsikrika
Information Technologies
Institute
Centre for Research and
Technology Hellas
6th Klm Charilaou-Thermi Rd
Thessaloniki, 57001, Greece
E-mail:
theodora.tsikrika@iti.gr

Stefanos Vrochidis
Information Technologies
Institute
Centre for Research and
Technology Hellas
6th Klm Charilaou-Thermi Rd
Thessaloniki, 57001, Greece
E-mail: stefanos@iti.gr

Una Williamson
Police Service of Northern Ireland
E-mail:
Una.Williamson@psni.pnn.police.uk

REFERENCES AND SOURCES

Andreadis, S., Gialampoukidis, I., Kalpakis, G., Tsikrika, T., Papadopoulos, S., Vrochidis, S., & Kompatsiaris, I. (2017). "A Monitoring Tool for Terrorism-related Key-players and Key-communities in Social Media Networks." In Proceedings of the IEEE European Intelligence and Security Informatics Conference (EISIC 2017), p. 166.

Andrews, S. (2011). "In-close2, a high performance formal concept miner." In Conceptual Structures for Discovering Knowledge, Proceedings of the 19th International Conference on Conceptual Structures (ICCS 2011), pp.50-62.

Association of the Chiefs of Police Officers (2013). "Online research and investigation." College of Policing. Available at: http://library.college.police.uk/docs/appref/online-research-and-investigation-guidance.pdf [Accessed 21 Aug. 2017]

Auer, S., Bizer, C., Kobilarov, G., Lehmann, J., Cyganiak, R., & Ives, Z. (2007). "DBpedia: A nucleus for a Web of open data." The Semantic Web, pp. 722-735.

Baker, C. F., Fillmore, C. J., & Lowe, J. B. (1998). "The Berkeley FrameNet project." In Proceedings of the 36th Annual Meeting of the Association for Computational Linguistics (ACL 1998) and 17th International Conference on Computational Linguistics (COLING 1998), Volume 1, pp. 86-90.

Ballesteros, M., Bohnet, B., Mille, S. & Wanner, L. (2014). "Deep-Syntactic Parsing." In Proceedings of the 25th International Conference on Computational Linguistics (COLING 2014), pp. 1402-1413.

Basic Law for the Federal Republic of Germany in the revised version published in the Federal Law Gazette Part III, classification number 100-1, as last amended by Article 1 of the Act of 23 December 2014 (Federal Law Gazette I p. 2438).

Blondel, V. D., Guillaume, J. L., Lambiotte, R., & Lefebvre, E. (2008). "Fast unfolding of communities in large networks." Journal of Statistical Mechanics: Theory and Experiment, vol. 2008, no. 10, p. P10008.

Bohnet, B. & Nivre, J. (2012). "A transition-based system for joint part-of-speech tagging and labeled non-projective dependency parsing." In Proceedings of the 2012 Joint Conference on Empirical Methods in Natural Language Processing and Computational Natural Language Learning (EMNLP-CoNLL 2012), pp. 1455–1465.

Bohnet, B., Mille, S., Favre, B., & Wanner, L. (2011). "<StuMaBa>: from deep representation to surface." In Proceedings of the 13th European workshop

on Natural Language Generation (ENLG 2011), Surface-Generation Shared Task, pp. 232-235.

Bouchard, M., Joffres, K., & Frank, R. (2014). "Preliminary analytical considerations in designing a terrorism and extremism online network extractor". In Computational Models of Complex Systems, pp. 171-184.

BOE-A-1999-23750 (1999). "The Data Protection Act Law (Ref. BOE-A-1999-23750)". [online] Available at http://www.boe.es/buscar/doc.php?id=BOE-A-1999-23750 [Accessed 21 Aug. 2017]

Cavoukian, A. (2011). "Privacy by Design The 7 Foundational Principles". Information and Privacy Commissioner of Ontario. [online] Available at: http://www.privacybydesign.ca/ [Accessed 21 Aug. 2017]

Chen, H. (2011). "Dark Web: Exploring and data mining the dark side of the Web," Vol. 30. Springer Science & Business Media.

Clauset, A., Newman, M. E., & Moore, C. (2004). "Finding community structure in very large networks," Physical Review E, vol. 70, no. 6, p. 066111.

Code of Criminal Procedure in the version published on 7 April 1987 (Federal Law Gazette [Bundesgesetzblatt] Part I p. 1074, 1319), as most recently amended by Article 3 of the Act of 23 April 2014 (Federal Law Gazette Part I p. 410).

Danon, L., Diaz-Guilera, A., Duch, J., & Arenas, A. (2005) "Comparing community structure identification," Journal of Statistical Mechanics: Theory and Experiment, vol. 2005, no. 09, p. P09008.

Diligenti, M., Gori, M., & Maggini, M. (2004). "A unified probabilistic framework for eb page scoring systems."" IEEE Transactions on Knowledge and Data Engineering, vol. 16, no. 1, pp. 4–16.

Furche, T., Gottlob, G., Grasso, G., Schallhart, C., & Sellers, A. (2013). "OXPath: A language for scalable data extraction, automation, and crawling on the Deep Web." The VLDB Journal, 22(1), 47-72.

Ganter, B. & Wille, R. (1998). "Formal Concept Analysis: Mathematical Foundations", Springer-Verlag, Berlin.

Germany, Customs Investigation Service Act (Zollfahndungsdienstgesetz), 16 August 2002, last amended 20 June 2013. [online] Available at: http://www.gesetze-im-internet.de/zfdg/BJNR320210002.html [Accessed 21 Aug. 2017]

Gialampoukidis, I., Kalpakis, G., Tsikrika, T., Papadopoulos, S., Vrochidis, S., & Kompatsiaris, I. (2017). "Detection of Terrorism-related Twitter Communities using Centrality Scores." In Proceedings of the 2nd International Workshop on Multimedia Forensics and Security, pp. 21-25.

Gialampoukidis, I., Kalpakis, G., Tsikrika, T., Vrochidis, S., & Kompatsiaris, I. (2016a). "Key player identification in terrorism-related social media

networks using centrality measures." In Proceedings of the IEEE European Intelligence and Security Informatics Conference (EISIC 2017), pp. 112-115.

Gialampoukidis, I., Tsikrika, T., Vrochidis, S., & Kompatsiaris, I. (2016b). "Community Detection in Complex Networks Based on DBSCAN* and a Martingale Process." In Proceedings. of the 11th IEEE International SMAP Workshop, pp. 1-6.

Great Britain (1998), Data Protection Act. London: Stationery Office. [online] Available at: http://www.legislation.gov.uk/ukpga/1998/29/contents [Accessed 21 Aug. 2017].

Great Britain (2000), Regulation of Investigatory Powers Act. London: Stationery Office. [online] Available at: https://www.legislation.gov.uk/ukpga/2000/23/contents [Accessed 21 Aug. 2017].

Hajič, J., Ciaramita, M., Johansson, R., Kawahara, D., Martí, M. A., Màrquez, L., Meyers, A., Nivre, J., Padó, S., Štěpánek, J., Straňák, P., Surdeanu, M., Xue, N., & Zhang, Y. (2009). "The CoNLL-2009 shared task: syntactic and semantic dependencies in multiple languages." In *Proceedings of the Thirteenth Conference on Computational Natural Language Learning: Shared Task* (CoNLL 2009), pp. 1-18.

He, Y., Xin, D., Ganti, V., Rajaraman, S., & Shah, N. (2013). "Crawling Deep Web entity pages." In Proceedings of the 6th ACM international conference on Web Search and Data Mining (WSDM 2013), pp. 355-364.

Hellenic Parliament (1951), Penal Code.

Hellenic Parliament (1994), For the protection of free correspondence and communication and other provisions.

Hellenic Parliament (2003), Article 251 of the Criminal Procedure Code.

Hellenic Parliament (2004), Article 253A of the Criminal Procedure Code.

Hellenic Parliament (2008), The Constitution of Greece, as revised by the parliamentary resolution of May 27th 2008 of the VIIIth Revisionary Parliament.

Interpol (2017). "Crimes against children, victim identification." Interpol. [online] Available at: https://www.interpol.int/Crime-areas/Crimes-against-children/Victim-identification [Accessed 21 Aug. 2017].

Kravitz, D. W. (1993). U.S. Patent No. 5,231,668. Digital signature algorithm. Washington, DC: U.S. Patent and Trademark Office.

Lancichinetti, A., Fortunato, S. & Radicchi, F. (2008) "Benchmark graphs for testing community detection algorithms," Physical Review E, vol. 78, no. 4, p. 046110.

Langheinrich, M., (2001). "Privacy by design – principles of privacy-aware ubiquitous systems." In Proceedings of the Third International Conference on Ubiquitous Computing (Ubicomp 2001), pp. 273-291.

Leach, P. J., Mealling, M., & Salz, R. (2005). "A universally unique identifier (UUID) URN namespace". Available at: https://tools.ietf.org/html/rfc4122 [Accessed 21 Aug. 2017].

National Police Chief Council (2015). "NPCC Guidance on Open Source Investigation / Research". Kent and Essex Police. https://www.suffolk.police.uk/sites/suffolk/files/003525-16_npcc_guidance_redacted.pdf [Accessed 1 October 2017]

Kingsbury, P. & Palmer, M. (2002). "From TreeBank to PropBank." In Proceedings of the Third International Conference on Language Resources and Evaluation (LREC 2002), pp. 1989-1993.

Manning, C. D., Surdeanu, M., Bauer, J., Finkel, J. R., Bethard, S., & McClosky, D. (2014). "The Stanford CoreNLP Natural Language Processing Toolkit". In Proceedings of the 52nd Annual Meeting of the Association for Computational Linguistics (ACL 2014) - System Demonstrations, pp. 55-60.

Mel'čuk, I. (1988). "Dependency Syntax: Theory and Practice." State University of New York Press, Albany.

Mille, S., Carlini, R., Burga, A. & Wanner, L. (2017a). "FORGe at SemEval-2017 Task 9: Deep sentence generation based on a sequence of graph transducers." In Proceedings of the 11th International Workshop on Semantic Evaluation (SemEval-2017), pp. 920-923.

Mille, S., Carlini, R., Latorre, I. & Wanner, L.. (2017b). "UPF at EPE 2017: Transduction-based Deep Analysis." In Proceedings of the 2017 Shared Task on Extrinsic Parser Evaluation (EPE 2017), pp. 80-88.

Mille, S. & Wanner, L. (2015). "Towards large-coverage detailed lexical resources for data-to-text generation." In Proceedings of the first workshop on data to text generation.

Miller, G. A. (1995). "WordNet: a lexical database for English." Communications of the ACM, vol. 38, no. 11, pp. 39-41.

Ministerio de Gracia y Justicia (2015), Criminal Procedure Law (approved by Royal Decree of September 14, 1882, and amended up to Organic Law No. 13/2015 of October 5, 2015) (Ref. BOE-A-1882-6036). Available at: http://www.wipo.int/wipolex/en/details.jsp?id=16706 [Accessed 21 Aug. 2017]

Ministerio de Justicia-Secretaria General Tecnica (2013), Criminal Code.

McCulloch, H. (2007) "International Child Sexual Exploitation Image Database". ICPO Interpol. [online] Available at: http://cf.cdn.unwto.org/sites/all/files/docpdf/21sttaskforcemeetingreport2007novmcculloch.pdf [Accessed 21 Aug. 2017]

Navigli, R. & Ponzetto, S. P. (2012) "BabelNet: The automatic construction, evaluation and application of a wide-coverage multilingual semantic network." Artificial Intelligence, vol. 193 pp. 217-250.

Petkos, G., Schinas, M., Papadopoulos, S., & Kompatsiaris, I. (2017). "Graph-based multimodal clustering for social multimedia." Multimedia Tools and Applications, vol. 76, no. 6, pp. 7897–7919.

PoliceICT (2017). "Security Open Standards." Metropolitan Police Service. Available at: https://ict.police.uk/national-standards/security/security-open-standards/ [Accessed 21 Aug. 2017]

P. Pons & M. Latapy, (2006) "Computing communities in large networks using random walks." Journal of Graph Algorithms and Applications, vol. 10, no. 2, pp. 191–218.

Prayudi, Y., & Sn, A. (2015). "Digital chain of custody: State of the art." International Journal of Computer Applications, vol. 114, no. 5.

Rand, W. M. (1971) "Objective criteria for the evaluation of clustering methods," Journal of the American Statistical Association, vol. 66, no. 336, pp. 846–850.

Schuler, K. K. (2005) "VerbNet: A broad-coverage, comprehensive verb lexicon." Ph.D. Dissertation. University of Pennsylvania, Philadelphia, PA, USA. AAI3179808.

Trottier, D. (2015). "Open source intelligence, social media and law enforcement: Visions, constraints and critiques." European Journal of Cultural Studies, vol. 18, no. 4-5, pp. 530-547.

Williams, J. D. (2012). "ACPO Good Practice Guide for Digital Evidence." Metropolitan Police Service.

Weninger, T., Palacios, R., Crescenzi, V., Gottron, T., & Merialdo, P. (2016). "Web Content Extraction: a MetaAnalysis of its Past and Thoughts on its Future." ACM SIGKDD Explorations Newsletter, vol. 17, no. 2, pp.17-23.

Zampoglou, M., Papadopoulos, S., & Kompatsiaris, I. (2017). "Large-scale evaluation of splicing localization algorithms for Web images." Multimedia Tools & Applications, vol. 76, no. 4, pp. 4801-4834.

Zhao, F., Zhou, J., Nie, C., Huang, H., & Jin, H. (2016). "SmartCrawler: A Two-stage Crawler for Efficiently Harvesting Deep-Web Interfaces." IEEE Transactions on Services Computing, vol. 9, no. 4, pp. 608-620.

Zhou, Y., Qin, J., Lai, G., Chen, H., & Reid, E. (2005). "Building knowledge management system for researching terrorist groups on the Web." In Proceedings of the 11th Americas Conference on Information Systems (AMCIS 2005), pp. 344.

OSINT FROM A UK PERSPECTIVE: CONSIDERATIONS FROM THE LAW ENFORCEMENT AND MILITARY DOMAINS

Douglas Wells, MA Conflict, Development and Security Studies
CENTRIC (Centre of Excellence in Terrorism, Resilience, Intelligence and Organised Crime Research), Sheffield Hallam University, UK
Researcher

Helen Gibson, PhD
CENTRIC, Sheffield Hallam University, UK
Lecturer in Computing

Keywords: OSINT, law enforcement, military, intelligence

ABSTRACT

Both law enforcement and the military have incorporated the use of open source intelligence (OSINT) into their daily operations. Whilst there are observable similarities in how these organisations employ OSINT there are also differences between military and policing approaches towards the understanding of open source information and the goals for the intelligence gathered from it. In particular, we focus on evaluating potential similarities and differences between understandings and approaches of operational OSINT between British law enforcement agencies and UK based MoD researchers and investigators. These observations are gathered towards the aim of increasing interoperability as well as creating opportunities for specific strengths and competencies of particular organisational approaches to be shared and utilised by both the military and law enforcement.

1. INTRODUCTION

The value of intelligence, be it for law enforcement, the military, or businesses, cannot be understated. Intelligence gives an organisation some kind of advantage over another; this might be the vital intelligence that solves a crime, enables victory in a battle, or allows a company to return a better profit than their rivals. This intelligence may come from a wide range of sources: from people who have been interviewed, from internal data and logs, from crime scene evidence, from videos and imagery, from phone calls and communications, and many more besides. One intelligence discipline that is attracting more and more attention is open source intelligence (OSINT). Fuelled by the near ubiquitous nature of the internet and coupled with narcissistic tendencies that have accompanied the rise in the use of social media, OSINT has moved into the fore of the intelligence gathering disciplines. However, as we will see in this paper social media is not the only source of open source intelligence and nor does it exist in a vacuum from other intelligence sources. This study is built primarily upon a qualitative analysis but also references personal communications of interactions between the researchers and key informants of the military and police OSINT sector.

2. DEFINING OSINT

Open Source Intelligence will be shown throughout this paper to be a dynamic term that often consists of contradictory or ambiguous pre-requisites and thus one single definition does not exist. A good starting point is the definition provided by the CIA (2010) who make the claim that "information does not have to be secret to be valuable" and build on this tenet to describe OSINT as public information that can be retrieved from:

- The Internet
- Traditional mass media (e.g., television, radio, newspapers, magazines)
- Specialised journals, conference proceedings, and think tank studies
- Photography
- Geospatial information (e.g. maps and commercial imagery products)

However, they do not rule out the fact that other open sources may also be available as well as clarifying that this data collected from 'publically available' sources must be used in an 'intelligence context' and the collection of the subject data may be performed in an overt manner.

The Ministry of Defence (2011) in the UK provides a more specific definition of OSINT: "intelligence derived from publicly available information that has limited public distribution or access." In particular, they state that OSINT material is especially useful when "exploited by trained analysts to ensure the intelligence produced is unbiased and free of prejudice, open-source material is no less important than protectively marked material". This statement of OSINT being equal to other forms of intelligence is a recurring theme within official doctrine around OSINT; however, many of these reports also mention that it sometimes can have difficulty in being taken seriously.

Most intelligence domains (HUMINT, SIGINT, IMINT, etc.) have their roots in the military and in such a context; OSINT became an accepted term around the mid-90s (Steele, 1995). An early example of OSINT was the Foreign Broadcast Intelligence Service (FBIS), which monitored

foreign radio broadcasts, transcribed and translated them, beginning in 1941. In fact, as early as 1947, Allan Dulles (formerly Head of the CIA), and at that point working for the Office of Strategic Services, is reported as saying that 80 percent of the required intelligence during peace time could potentially be obtained through open sources and more recent estimates have continued to offer the same claim or even higher (Gibson, 2014).

The National Police Chiefs Council (NPCC) in the UK also provides two similar definitions of open source (2015). The first being on what is considered open source research:

> *"the collection, evaluation and analysis of materials from sources available to the public, whether on payment or otherwise to use as intelligence or evidence within investigation".*

The NPCC then go on to define open source information as being:

> *"Open source is defined as publically available information (i.e., any member of the public could lawfully obtain the information by request or observation). It includes books, newspapers, journals, TV and radio broadcasts, newswires, Internet WWW, and newsgroups, mapping, imagery, photographs, commercial subscription databases and grey literature (conference proceedings and institute reports).*

Thus we see that the police definition of open source is somewhat more extensive and specific than what is supplied by the MoD. It could be argued that the NPCC definition is more detailed due to a recent publication, additionally, following the Snowden and Assange leaks of 2013-2016 (Kwoka, 2015, p.1387), it may have been of interest to better define online investigation tactics to avoid potential controversy and increase public transparency (ISC, 2015, p.6). Therefore, because the NPCC definition is more recent and more developed, yet doesn't conflict or disagree with current UK military practices, this paper will use it as the primary definition of OSINT for subsequent comparisons.

Descriptions of OSINT, such as those cited from the CIA, MoD, and NPCC, characterise the range of definitions available of OSINT and their tendency to be rather broad and nonspecific. And while there may

be areas of agreement within these definitions and others; it is also clear that some of the generic criteria for defining OSINT may be somewhat ambiguous. As such there are at least three observable areas of potential dispute: (1) the use of the term *publically available;* (2) the extent to which the data is collected *overtly* and *covertly*; and (3) the requirement to practice good *cyber-hygiene* when conducting open source investigations. We now consider these points term-by-term.

Firstly, the phrase *'publically available'* is open to interpretation. Both military and law enforcement officers may, when authorised, draw upon 'open source' data that a non-service civilian could not gain access to. Two such examples include; driver and vehicle registrations (DVLA databases) and financial data including credit ratings and banking providers (Home Office Centre for Applied Science and Technology (CAST), 2016, personal communication, November 2016). Although such databases can be accessed by paying customers, local authorities and police organisations this information is not made available to the general public. Indeed, there may be some debate as to whether such access to data can reasonably be considered 'open source'. Whilst information stored by websites such as 192.com holds personal OSINT data behind 'paywalls', this is considered to be 'fair game' meaning anyone with the interest in purchasing details such as personal addresses, electoral and telecoms data may do so. Indeed, other databases, such as those maintained by large companies often host what is known as 'consented data'; and, while such data is only stored when someone gives their consent, the extent to which they are made aware of both how this data may be used in the future and opportunities to scrub data from these records are not expressly advertised. Arguably, police and military access to DVLA and financial databases are a step beyond 'paywalls', wherein the data is not available for the wider public under any circumstance.

Secondly, although many OSINT definitions describe that the data collection process *may* be done in an overt manner, in practice it is rarely done so (South Yorkshire Police, Digital Media Investigations Officer, 2017, personal communication, February 2017). This is especially true due to the dominance of the internet both for data storage as well as through its convenience to search and locate intelligence through social media and other publicly open sites, and while the NPCC defines five levels of open source research, only Level 1 is explicitly termed overt research (National Police Chiefs Council, 2015).

Social media especially is a minefield because of the personal nature of almost all information posted to such sites. For example, considering investigations that operate on Twitter and Facebook, users are not and cannot be notified if their profile content is being reviewed, screen-captured, directly downloaded by another user or through a specially designated OSINT software product such as Repknight (2017), Echosec (2017) and Cosain (2017). Interestingly, such OSINT products market themselves specifically for Policing, Home Office and MoD usage by making themselves on the G-Cloud (the UK government's digital marketplace (see e.g., Cosain[1] and Palantir[2])).

Historically and internationally, such methods of covert OSINT surveillance may be recognised as early as the 1930's, in which the aforementioned United States Foreign Broadcast Intelligence Service (FBIS) (Mercado, 2007) was established to begin monitoring overseas public radio frequencies, by 1941 it had begun to turn radio into a primary intelligence source during World War II. In a similar manner to the investigation methods of the contemporary era, this OSINT was accessing publicly available sources through covert technologies with trained analysts, the process was invisible to axis powers (Mercado, 2001) in the same manner modern social media collection may be undetectable to suspect user profiles.

Thirdly, often not stated is the responsibility of military and law enforcement (when operating at levels 2-5, see below) to act with high levels of 'cyber hygiene', minimising the digital footprint left behind on websites, or use services to mask such a presence. This approach is considered to be more of a counter-intelligence measure than clandestine exploitation. Indeed, it is often necessary to protect the anonymity of investigators, the organisation as well as the individuals or groups being targeted, which may in turn reveal details of the operation.

Additionally, UK law enforcement have specific guidance, via the College of Policing, detailing the requirements for level 4-5 OSINT investigations utilising social media account takeovers and covert human intelligence sources (CHIS) to obtain 'open source' social media evidence

[1] https://www.digitalmarketplace.service.gov.uk/g-cloud/services/945108024310388 (Cosain)

[2] https://www.digitalmarketplace.service.gov.uk/g-cloud/services/388738118169964 (Palantir Front Line Policing and Intelligence)

or intelligence (Cleveland Police, 2014). This may be a particularly contentious issue, due to the high-level covert tactics taken to impersonate or infiltrate online sites in the pursuit of data acquisition. They would appear to contradict any overt possibilities of OSINT as well as massively stretching definitions of what is deemed 'publicly available'. As such, levels 4-5 of OSINT usually require the highest levels of surveillance authority in place (National Police Chiefs Council, 2015; Home Office, 2014). These levels are generically accepted to be:

1. Overt OSINT Investigations/Research
2. Core OSINT Investigation/Research
3. Covert Advanced OSINT Investigation/Research
4. Covert Internet and Networks Investigations
5. Undercover Online/Covert Internet Investigator

Level 5 OSINT deployment is of particular interest, because it appears to blur the line between OSINT and covert surveillance and interception the most. It is defined as;

> *"Online covert activity 4.32 The use of the internet may be required to gather information prior to and/or during a CHIS operation... the CHIS may need to communicate online, for example this may involve contacting individuals using social media websites. Whenever a public authority intends to use the internet as part of an investigation, they must first consider whether the proposed activity is likely to interfere with a person's Article 8 rights, including the effect of any collateral intrusion. Any activity likely to interfere with an individual's Article 8 rights should only be used when necessary and proportionate to meet the objectives of a specific case. Where it is considered that private information is likely to be obtained, an authorisation (combined or separate) must be sought as set out elsewhere in this code." (National Police Chiefs Council, 2015; Home Office, 2014).*

The above three contradictions show that many existing definitions of OSINT are somewhat ambiguous when considering the technical practicalities of both contemporary law enforcement and military approaches. It may be of interest to explore whether these definitions are kept deliberately vague to allow the optimal access to investigative equipment, tactics and data sources.

3. INTEGRATION OF OSINT AS AN INTELLIGENCE DISCIPLINE

Despite the military being one of the key proponents of the use of OSINT, both from the US and also NATO (who produced the de facto OSINT handbook in 2001) the extent to which open source information is used in military operations is underreported with, perhaps unsurprisingly, few examples in the public domain. Nevertheless, there are continued efforts to push forward the use of OSINT in combination with data mining techniques as well as text analytics and artificial intelligence as a solution to enhance the capabilities of intelligence analysts. Such analyses are now feasible and, in fact, demanded due to the growing availability of real-time and predictive analytics which can utilise information from the past and present and use it to predict what may happen in the future (McCue, 2014).

Although OSINT has merits of its own as a single intelligence source, particularly in the military domain it can also be used to validate information garnered from closed intelligence sources and as such may enable the protection of a closed source though obtaining the same information from an open one. OSINT can also be utilised as part of an 'all-source analysis' bringing further credibility to the intelligence as it has been verified through multiple sources (Haigler, 2012).

In the near future, it is expected that the use of OSINT within the military will only increase simply due to the amount of information being made available online, the ease with which it can be accessed, the relatively low-cost of obtaining it compared with other intelligence sources as well as counteracting the feeling of not being left behind (i.e., everyone else is doing it) (Homeland Security Research, 2017)

Due to the UK police's reliance on OSINT to help provide evidence as well as enhance and parallel evidence from other sources, it may be argued as to having a greater structure and focus than in the military, partially due to the greater reliance on capturing evidence and the requirement for such evidence to stand up reliably in court when called upon.

In many cases, obtaining open source intelligence may be considered a form of directed surveillance, when conducted at level two and above in the aforementioned levels of open source research. In order to carry out such an investigation the police and the specific case in question is authorised via a directed surveillance authority (DSA). Such a permission may be given by "... an authorising officer where he or she believes that the authorisation is necessary in the circumstances of the particular case on the grounds that it is: (a) in the interests of national security; (b) for the purpose of preventing or detecting crime or of preventing disorder; (c) in the interests of the economic well-being of the UK; (d) in the interests of public safety; (e) for the purpose of protecting public health" (Home Office, 2014)

Such legislation may appear to further muddy the definitions of OSINT, as levels 2+ of OSINT investigative deployment appear to require 'covert surveillance authorities' to be in place and set the conditions and limitations of the operation (with the exception of imminent threats to life or serious bodily harm). This may appear to the wider public as somewhat ambiguous for the collection of open or publicly available data, but is specifically to protect privacy via the *means of collection*. To ensure that data and evidence is captured in the correct open source manner, the JAPAN principles are still deemed by law enforcement as a suitable approach for OSINT analysts and officers (Kent Police, 1998). JAPAN is an acronym for **J**ustified, **A**uthorised, **P**roportionate, **A**uditable, **N**ecessary; and such an approach ensures that the values of the 1998 Human Rights Act are preserved (UK Government, 1998), most noticeably (Article 8) privacy, and to ensure everyone is treated with fairness and respect.

Military OSINT operations and intelligence have the benefit of being able to work from the UK remotely, assisting in operations across the globe. However this still means they are bound by RIPA (Regulation of Investigatory Powers Act) (UK Government, 2000) the same as UK police forces. There is not necessarily a requirement for the MoD to apply RIPA when conducting intelligence operations overseas; however, it is MoD policy to apply RIPA to any intelligence operation regardless of the country the intelligence is being gathered in citing the fact that "... [RIPA] provides a well-established regulatory framework for such operations and reduces the chances of improper conduct and abuse" (British Army, 2009). Nonetheless, from an outsider's perspective it is impossible to be certain how rigorously this mandate is being applied.

Particularly in the world of OSINT the application of RIPA can be problematic given that online investigations and specifically those on social media, which are becoming ever more common, are not sufficiently covered by RIPA (Bartlett et al., 2013) as it was written prior to the massive SM explosion from 2007 onwards (Digital Trends, 2016). Thus the sooner that all legislation can catch up with the growth of technology the more protection there will be for those who are utilising OSINT and those who are being investigated.

4. RELIABILITY OF OSINT

Open source information, in the UK the policing 5x5x5 grading system, tends to never be considered better than E41 Intelligence. E41 stands for an untested source, of which the reliability cannot be judged but it can be disseminated within the UK Police Service and to other law enforcement agencies as specified (College of Policing, n.d.).

Open source intelligence, is usually defined as being: "Open sources of information are widely available but may not be accurate, reliable or valid. The main uses of open-source information are to:

- Develop an understanding of the locations relevant to a piece of analysis
- Identify the potential impact of social and demographic changes
- Identify external factors that may impact on crime, disorder and community concerns
- Support and develop investigations by indicating lines of enquiry or corroborating other information
- Support the development of subject profiles and problem profiles.

There are several factors to take into account when using open-source information:

- Access may require the user to register or pay a fee (eg, online news media, the electoral roll)
- The use of open-source information should be audited
- The effect of local security policies on access to open-source information (eg, some sites are not available to local users)
- It is not subject to the same quality standards as closed sources
- It should be corroborated by supporting information

When accessing open-source information online, a footprint identifying the police address is left on the website. A non-attributable IT identity is sometimes required to avoid law enforcement being identified as the originator of the enquiry. An accredited covert internet investigator should be asked to advise in these instances." (College of Policing, 2013)

This is the same for both military and police classifications, whilst OSINT is seen as valuable, it is best through 'paralleling' or 'clustering' techniques. Paralleling is the process of using alternative research/investigative resources (such as OSINT) to find exact or associated information that has come from a closed source (Donohue, 2015). This is particularly useful for preserving the integrity and security of hidden and embedded assets, additionally this approach can be used to find and document a chain of evidence from intelligence leads.

Clustering, is a technique that utilises a collection of strong and, or, weak 'signals' to predict the bigger picture (Lesca and Lesca, 2011). For example, when trying to guess the end product of a recipe; the more individual ingredients that are learned, the greater the probability of understanding the specific type of cake. OSINT can be particularly useful for feeding in big data crawling results to help further validate or expand stronger human led analysis.

Paralleling is not the only use of OSINT though, and while many were still sceptical of open source information, the 9/11 attacks brought OSINT back to the fore in the military domain, as intelligence managers realised that such information could not be easily discounted (Hulnick, 2010). Post these attacks, researchers were even able to put together a network from open sources of the links between many of the hijackers and associates, thus leading to a better understanding of how the hijackers communicated and were able to remain undetected for long enough to carry out such an atrocity (Krebs, 2002). Thus despite the claims over its unreliability OSINT has proven itself to be useful not only for validating other intelligence, but also as an intelligence source in its own right. The onus is on the investigating analyst to have the training, knowledge and expertise to accurately assess the OSINT source individually and make a reasonable assumption about the reliability of the source on its own merits independent of whether it was obtained openly or not.

5. DIFFICULTIES AND DISPARITIES DEFINING OSINT IN MODERN SECURITY

As previously discussed there is not an accepted definition of open source intelligence be it for law enforcement, the military or elsewhere and even within existing definitions the scope of the material and the means that can be used to obtain it are not standardised and varies across different practices. This causes issues to new people entering the field as there is no standard reference or accepted form of OSINT. Even established books, such as Michael Bazzell's Open Source Intelligence Techniques (2016) include social engineering techniques that may not be considered acceptable for LEAs or military usage.

Law enforcement and the military may also collect OSINT for different reasons and we are at pains to point out the difference between OSINT for digital evidence capture and OSINT for intelligence capture.

As of June 2017, the UK military do not use the equivalents of CHIS or OSINT levels 4-5 in operations deemed open source intelligence or research gathering. Some exceptions to this may be 77th Brigade (British Army, 2017) who are known to use Facebook, Twitter and other social media to engage in non-lethal warfare (MacAskill, 2015). However, as a force wide security policy the majority of military OSINT does not involve any form of impersonation/engagement or CHIS approaches.

In gathering SM data, two primary types of profiles may be deployed; 'grey man' and 'embedded' accounts. (Nottinghamshire Police Open Source Intelligence Investigator, 2016, personal communication, August 2016). Grey man accounts are necessary to pass through the basic 'log in' requirements of SM sites such as Facebook, VK and Telegram, allowing the account access to a greater degree of content, than if the investigator wasn't registered with the site. These grey man accounts do not 'befriend, follow, or engage' in any form of communication with other profiles, their benefit is to simply pass through SM site login barriers to obtain open source content within. This approach is commonly used by the MoD and other non-policing governmental actors as they are considered to be deployed at OSINT levels 1-2. Beyond this, 'embedded

accounts' may be used (usually within law enforcement with regards to a specific tasking and a DSA). Such accounts are deliberately presented and maintained as genuine users, with friend lists, active statuses, profile interests, etc. These are designed to enable the profile to 'infiltrate private groups inside SM provider sites, or to gain access to suspect profiles with a greater degree of security. The specifics of how and to what extend such profiles are populated and integrated into social media networks is dependent on the localised force policy in the police.

In using OSINT for investigations both the military and the police have to tread a fine line around perception and how this impacts on the privacy of those who are under investigation. Furthermore, there is a blurring of lines between HUMINT and OSINT (particularly when dealing with crowdsourcing intelligence) (Mak et al., 2017). This concern would also be present when police or military extrapolate investigations and operations to third parties or outside experts.

There are also wider growing concerns around the expectations of privacy online ranging from the mantra that online privacy is dead and that those who are worried about exposing their personal details should just 'get over it' to legitimate concerns (Edwards and Urquhart, 2016). As the GDPR (General Data Protection Regulation) comes into force this also raises concerns around the access and storage of personal data; although, there are exceptions around law enforcement. Further confusing the issue are the complications that will arise as the UK looks to leave the EU and implements its own legislation away from existing EU law (O'Sullivan, 2017).

6. DIFFERENCES BETWEEN UK LAW ENFORCEMENT AND MOD USE OF OSINT:

6.1 Priorities for counterintelligence and OSINT leakage are different between the military and police

In UK law enforcement, ACPO (Association of Chief Police Officers), now formally known as the NPCC (National Police Chiefs Council), laid a foundation for online and social media privacy standards for police staff in their 2013 document: Guidelines on the Safe Use of the Internet and Social Media by MDP Officers (Ministry of Defence Police, 2013), officers are encouraged to use the internet for social media purposes, but insist that because *information on SM may be made public* they ought to behave as they would *on duty* given that "Information placed on the Internet or social media could potentially end up in the worldwide public domain and be seen or used by someone it was not intended for, even if it was intended to be 'private' or is on a closed profile or group. It is likely that any information placed on the Internet or social media will be considered to be a public disclosure." In this document, it is worth noting that Section 6 relates to: Safeguarding Personal and Sensitive Data which reiterates the requirement for police not being able to leak or disclose others' personal and private data, whilst Section 7 relates directly to preserving the integrity of the police force reputation.

Section 8**,** of the same document, is entitled: 'Keeping your private life private'. Due to the potential for criminals and malicious actors to use the internet, particularly social media to identify personal information about police officers. They may be capable of obtaining; 'embarrassing, discrediting, harassing, corrupting or blackmailing them or their families'. Therefore the guidance to "Ensure privacy settings for social media are set to the highest level, not to register on social media using pnn.police.uk e-mail addresses, to be careful when accepting 'friends' to access their social media, not to be associated with inappropriate material on 'friends' social media, not to be associated with social media of criminals and not to be associated with the social media of persons involved in serious organised crime." are issued to all officers governing their use of social media overall, (Derbyshire Police, 2012).

Furthermore, officer are encouraged not to post online specific details such as employer, job post, hobbies and locations frequented, images in uniform, mobile numbers and email addresses, vehicle and home addresses, family member details, etc. Additionally; "It is also recommended that police officers who may wish to pursue duties in covert policing carefully consider whether the publication of personal images and information on social media may restrict their future career opportunities in such areas on the grounds of personal safety, public safety and operational security."

The MoD has published similar standards in the; 'Online Engagement Standards' document of 2009 (Ministry of Defence, 2009). This document covers the same areas as UK law enforcement, however arguably with greater detail and is stricter with organisational and operational data security. Military personnel are encouraged to never speak as if they are doing so on behalf of their organisation without oversight from a senior commanding officer. Additionally, they should avoid publishing material that:

- Relates to operations or deployments
- Offers opinions on wider Defence and Armed Forces activity, or on third parties without their permission
- Attempt to speak, or could be interpreted as speaking, on behalf of your Service or the MoD
- Relates to controversial, sensitive or political matters

Additionally, it is advised that; "Such online presences provide an opportunity for Service and MoD civilian personnel to explain their work. But they also carry risks to individuals, to their Service and to Defence. Service and MoD civilian personnel are already using online presences and Defence information is entering the public domain unofficially. Guidelines are therefore required." This shows that there is a greater emphasis on security due to the increased security risks to individual personnel, the wider organisation, as well as in the data itself - which may be used by belligerent nations with a far greater skillset than the average 'criminal organisation'. Such personal data may give away operational and tactical intelligence such as vehicles and munitions, coordinates, time and date, movements, number of associates, ranks and specialisations.

Such data has recently been observed being publicised by journalists and military analysts relating to alleged Russian involvement in the Crimea. Indeed, the Russian soldier; Alexander Sotkin, nicknamed 'Sergeant Selfie', was ridiculed and criticised for seemingly leaking his geolocation and interior of his armoured signals vehicle publicly on Instagram (Gallagher, 2014). Although there is some debate as to the whether the geolocation (which appears to show activity across the border in Ukraine) is accurate, but nonetheless the incident caused a degree of international controversy, additionally with the individual in question being allegedly stripped of his rank as sergeant. Further social media embarrassments have been reported against U.S military families who received fake orders to leave South Korea. US Army counterintelligence are investigating the incidents of late September 2017 in which fake social media and mobile alerts were sent out; "warning American military families and Defense Department personnel of orders to evacuate the volatile peninsula" (Lamothe, 2017).

In the UK, armed forces are able to operate closed social media groups, such as restricted, private Facebook groups to inform family members about a group's well-being when oversees on campaigns with little internet connectivity, or, with a high level of secrecy involved (Royal Navy, 2017). It is likely such SM groups are the target of belligerent states for espionage and sabotage such as in the case of Alexander Sotkin's data leakage and the South Korean military family's hoax. Such incidents are taken very seriously from a military point of view as they may hint towards serious counterintelligence vulnerabilities, allowing for manipulation, espionage and disinformation campaigns to work effectively against operations, personnel and even target family members.

6.2 Usage of the Dark Web

As of early 2017, open source investigation sectors of the military did not officially classify the Dark Web as an 'open source' resource (Pattar, 2017), this decision is currently paralleled elsewhere the HMRC who also usually operate at open source levels 1-2 and do not access dark web URLs. Whilst this is in part due to security and infrastructure constraints, it has been recognised to be somewhat problematic and will

likely change in the foreseeable future. In particular OSINT investigators within the military may recognise the wealth of potential to investigate Dark Markets for associations towards funding terrorist groups and other foreign threats (Weiman, 2016).

It may be argued that the priorities of open source access to the dark web are different between the UK military and law enforcement agencies. In addition to terrorist, enemy state and other foreign concerns, UK police operations focus on leading priorities such as; child sexual exploitation (CSE), drug trafficking, online fraud and scamming communities, money laundering and various other organised criminal network forums and dark marketplaces (Buxton and Bingham, 2015; Home Office, 2017). Particularly, the strong focus on fighting CSE has encouraged an essential need for police officers and analysts to operate on the dark web as clarified by the HMIC (Her Majesty's Inspectorate of Constabulary) in 2017: "*The dark net provides abusers with a means of distributing indecent images of children around the globe to those who share their interest. It has provided an opportunity for such offending to be undertaken more widely. It has made the job of the police service and other agencies responsible for safeguarding children more difficult.*" The perceived anonymity, capacity to mask IP addresses and geolocation, as well as the difficulty of searching and penetrating dark net 'friend circles' has made it essential for law enforcement to pursue suspects and offenders on Tor and similar dark web browsers.

Further surrounding the topic of OSINT and CSE; a particular area of growing controversy and debate in the UK is for law enforcement dealing with such E41/Hearsay intelligence from the rise in popularity of 'paedophile hunter' vigilante groups such as; Guardians of the North (2017), The Hunted One (2017) and Dark Justice (2017). Such groups often impersonate underage children upon social media sites, but also utilise mobile messaging and dating applications such as Kik, Badoo, Snapchat, and WhatsApp.. The majority of paedophile hunter 'stings' utilise the described OSINT investigation levels 4 and 5. Indeed, the actions of paedophile hunter groups amount to OSINT SM account takeovers as well as online CHIS, these are carried out without a DSA or legal authorisation and provided to law enforcement. Whilst the police may make use of such intelligence and use paralleling techniques to capture their own evidence, this approach has come under significant criticism, both

internally within the force as well as externally for encouraging 'vigilantism' and dangerous practices with little or no concern for suspects to be mistaken, entrapped and publicised from amateur and possibly fallible investigative techniques (Perraudin, 2017).

Such concerns are not observably present in the media concerning military intelligence measures, nor are they likely to be treated with as much concern as law enforcement does. This is primarily due to the military's 'foreign facing' scope, (with the exception of national security threats such as terrorism), it is likely that such E41 intelligence obtained from a similar process about military interests would be treated as valuable, or at least worth researching or investigating further. Indeed, there exist many amateur OSINT online publications of interest to the MoD, some examples being bloggers that record and report on the movements of battleships near their coastal homes, journalists who carry out OSINT research into topics such as the aforementioned Russian military movements, but also into the analysis of publications and propaganda material of terrorist groups (e.g., Bellingcat, 2017).

The comparative reduction of the UK judicial systems involvement in the military collecting of intelligence for operational and tactical usage allows them a greater degree of freedom than having to pursue a chain of evidence for suspect conviction. Furthermore, this may in turn reduce the manual workload required by investigating and authorising officers and analysts.

6.3 Utilisation of External Advisors and Support

UK law enforcement often draws upon OSINT services through advice and direction from the Home Office's Centre of Applied Science and Technology (CAST). Products such as Cosain, Repknight and Echosec are listed through Home Office vetting and recommendations on an online 'portal' (CAST, 2017). Of these products, the majority are commercially engineered by the private sector as external developers, some of which are available for additional public and private workplaces. It has also been shown that law enforcement may get locked into certain products (e.g., Palantir) and there are concerns about background

information sharing that are barely acceptable at a law enforcement level but could be disastrous for a military operation, thus the tools utilised by the military must be carefully scrutinised before deployment (Harris, 2017).

While the military do make use of off-the-shelf tools they also utilise work with organisations to develop OSINT tools customised bespokely for military usage and are usually locked into being only available for them. The military ensures the signing of strict NDAs as well as secrecy agreements, the individuals developing products go through alpha and beta stages on site at military bases. Individuals working on them externally are usually required to have DV vetting (Ministry of Defence, 2017).

7. BENEFITS OF SHARING BEST PRACTICES BETWEEN DEFENCE AND LAW ENFORCEMENT

With regards to OSINT, law enforcement and the military often operate in the same space, utilising many of the same tools and techniques and thus may benefit from the experience of sharing best practices

7.1 Increased interoperability

With the future merger of the Home Office and MoD (DSTL) (Home Office, 2017b) it is likely in the future that the two organisations will increase their areas of overlap and collaboration on joint operations and intelligence sharing exercises. Therefore it would be beneficial to increase the resilience and capacity of both parties if feasible. Increasing interoperability of OSINT investigations and research towards a compatible system would allow for greater collaboration on overlapping areas. For example, considering concerns such as domestic terrorist threats, increased interoperability could in the case of OSINT, lead to increased police capability to parallel military intelligence, but more importantly, enhanced military procedures to investigate and research threats in a manner compatible with policing 'chain of evidence concerns'.

7.2 Enhanced rigour and chain of custody

It may be beneficial for military operations to begin a best practice of treating intelligence sources in a similar manner as the police do for evidence gathered on OSINT investigations. This includes protection of data (hashing), integrity of data in case it is needed as evidence or even to be posted publicly in case of criticism. Increasingly we are seeing media channels belonging to opposing nations utilising news reports in a negative propaganda fashion. Examples such as 'Russia Today' attempts to demoralise and criticise the UK and US through social, political and military reports (O'Sullivan, 2014; Johnson, 2016). Therefore, as all aspects of military and law enforcement are fair game for open criticism, it may be beneficial for military OSINT investigations and research

to embrace the evidence capture and auditing standards of the police force, perhaps embracing the JAPAN principles, this would provide fair justification of a reasonable and proportionate use of OSINT that would minimise the damage of triggering privacy and other human rights criticisms. Furthermore, by considering policing standards, there may be subsequent improvements in reviewing and managing open source analysts and researchers, particularly as good or bad intelligence leads could be traced back along the chain of evidence audit.

7.3 Improving security, personal and organisational counterintelligence standards

The contemporary digital age results in increasingly complex and strenuous taskings for counterintelligence military and security services. Whilst this is naturally a greater concern of the MoD, it may represent a best practice that the law enforcement may consider a horizon challenge to embrace today (Lord, 2015). Indeed, the high standards of confidentiality and security regarding counter intelligence and data leakage from the military perspective certainly aren't neglected or ignored by police guidance and best practices. However, there are notable differences with the inclusion of the media, particularly for documentaries and entertainment television, which seek to detail and even challenge state surveillance technologies (Channel 4, 2016). Such documentaries can be argued to enhance the police-public relationship through awareness and education in the interest of fostering greater communication and collaboration. This is perhaps a convenience the military does not need considering OSINT, as the UK public are rarely the subject of its investigations and operations. Therefore, this may allow a greater degree of secrecy for military analysts 'training, techniques and tactics' for locating and exploiting OSINT. It may be of value for the preservation of both military and policing open source practices to discuss, limit or reduce the number of law enforcement documentaries if they are deemed to be compromising valuable; tools, exploits and tactics.

As mentioned earlier in the MoD OSINT definition, there is a great emphasis on utilising trained analysts to optimise the usefulness and benefits of OSINT; "to ensure the intelligence produced is unbiased and

free of prejudice" (Ministry of Defence, 2011). Furthermore, the military place a great emphasis on developing OSINT tools and technologies in-house, this ensures that they have an immediate input to the development of open source products through Alpha and Beta development stages, as well as close contact to product contractors for quick and efficient training and software updates and patches.

7.4 Development of OSINT standardisation

Currently, different UK police forces apply different rules and best practices for the collection of data prior to achieving a DSA under RIPA (West Yorkshire Police Analyst 2017, personal communication 12 May). Some allow for a 'once over' single check of a profile, whereas others allow for up to, but no more than 3 looks at a unique profile (Sorinteq, 2017). Additionally, depending on the senior investigating officer (SIO) different approaches may be taken to acquire, or to work around a DSA (such as utilising a NOD, non-operational directive or getting a retrospective DSA). Whilst both the military and the College of Policing provide their own internal OSINT training packages, there are also a vast number of third party providers of OSINT training who are able to train both military and law enforcement in advanced open source analysis.

Much of the individual police officer and military analyst actions on an investigation or OSINT research job are dependent on the SIO (or Commanding Officer) leading the case, as well as upon the conditions specified in the Directed Surveillance Authority. As a result of this, OSINT investigative techniques, tools used, and working methodologies may be shared between different groups. It may be beneficial in the future to establish a wider set of standards and best practices that not only different military or individual police forces could use, but may also be used between military and law enforcement interchangeably.

CONCLUSION

In conclusion, UK police and military open source investigations from within the UK have a great deal of similarities; this is particularly due to them both being under the governance of RIPA (2000). However, there are several observable differences between the two organisations.

The first observable difference is in the handling of a chain of evidence between the two bodies. UK police forces often have to prioritise and integrate a chain of custody for any intelligence that may lead to prosecution or to be shown in a court of law. Therefore, the police tend to have a more structured and detailed approach to evidence gathering, for example following the JAPAN approach, that ensures intelligence is either processed or paralleled into a secure, auditable and useful format. As noted, the military may benefit somewhat from a similar system that could protect data integrity from public criticisms, as well as leading to greater management of researcher and analyst efficacy. Additionally, the military hold a greater capacity to act on E41 intelligence provided to them from external and untested sources, they face a lesser degree of public insight and subsequently potential criticism.

Secondly, there are noticeable differences between the use of third party software and developers. The UK MoD prioritise the use of bespoke software tools and in-house training solutions, often requiring DV security vetting for contractors to work on site and in association with them. Alternatively, law enforcement have traditionally used a variety of commercial and private sector solutions, some of which are specifically designed for police OSINT, however these are not developed with the same degree of bespoke and internal design.

Thirdly, there are differences with organisational approaches towards the dark web. As stated, currently the MoD have a far more cautious approach to operating on the dark web. As detailed, UK law enforcement have faced both pressure and necessity to operate in this domain, particularly due to police specific concerns such as online child sexual exploitation. It is likely however in the near future that the military will include the dark web as part of their open source domain. Therefore, it may be beneficial for the MoD to discuss merging best practices and standards that have been nurtured by contemporary policing approaches.

Additionally, there are slight observable differences between the military and policing structures in regards to counterintelligence. The MoD provide slightly stricter guidelines, particularly revolving around operational security, as such they also offer closed SM groups to provide direct information to families of serving members when they are restricted or not able to use SM personally. Furthermore, the military faces greater challenges of preserving intelligence from belligerent states as well as protecting its personnel and families from a higher severity of threat. As stated earlier, such concerns include disinformation campaigns which have been used internationally to disrupt and displace personnel and families.

Overall there are clearly more overlaps and similarities than differences. The observable differences are defined by either the relationship to judiciary and prosecution services, or through the severity of the risk and security level they operate at.

This document serves as a brief overview of observable differences between UK military and policing OSINT practices. A more in depth and detailed review would be ideal for formulating how, or why, these differences have occurred. In particular, envisioned next steps for future research may include; firstly identifying the extent of operational and tactical differences between the two organisations, and secondly; building a roadmap for mapping potential compatible best practices that may lead to greater interoperability (particularly when considering counter terrorism), organisational efficiency (primarily for military auditing and evidence capture), increased capability (such as military dark web best practices), and greater SM counterintelligence awareness (primarily for policing security).

Contacts:

Douglas Wells
CENTRIC
Sheffield Hallam University, UK
E-mail: d.wells@shu.ac.uk

Helen Gibson
CENTRIC
Sheffield Hallam University, UK
E-mail: h.gibson@shu.ac.uk

REFERENCES AND SOURCES

Bartlett, J., Miller, C., Crump, J., and Middleton, L., (2013). Policing in an Information Age. CASM Policy Paper. DEMOS. https://www.demos.co.uk/files/DEMOS_Policing_in_an_Information_Age_v1.pdf?1364295365

Bazzell, M. (2016) Open Source Intelligence Techniques: Resources for Searching and Analyzing Online Information. 5th Edition. CreateSpace Independent Publishing Platform

Bellingcat (2017) https://www.bellingcat.com/

British Army (2009) British Army Field Manual. Volume 1 Part 10: Countering Insurgency. London: Ministry of Defence.

British Army (2017) 77th Brigade. http://www.army.mod.uk/structure/42952.aspx

Buxton, J., Bingham, T., (2015). The Rise and Challenge of Dark Net Drug Markets. *Global Drug Policy Observatory*. Swansea University. https://www.swansea.ac.uk/media/The%20Rise%20and%20Challenge%20of%20Dark%20Net%20Drug%20Markets.pdf

CAST (2017). Centre for Applied Science and Technology. Home Office Security, Science and Innovation. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/619286/introduction-to-cast-jun2017.pdf

Channel 4 (2016). Hunted: How the fugitives were hunted. http://www.channel4.com/info/press/press-packs/hunted-how-the-fugitives-were-hunted

CIA (2010) INTelligence: Open Source Intelligence. *Central Intelligence Agency* https://www.cia.gov/news-information/featured-story-archive/2010-featured-story-archive/open-source-intelligence.html [Accessed 1 October 2017]

Cleveland Police (2014). Social Media and Electronic Communication Guidance. (pp.6-7.) https://www.whatdotheyknow.com/request/409672/response/1002847/attach/2/Guidance%20document.PDF.pdf [Accessed 1 October 2017]

College of Policing (n.d.) Authorised Professional Practice. How to complete a 5x5x5 form http://library.college.police.uk/docs/APPref/how-to-complete-5x5x5-form.pdf

College of Policing. (2013). Intelligence Management: Intelligence Collection, Development and Dissemination. https://www.app.college.police.uk/app-content/intelligence-management/intelligence-cycle/?s=intelligence#top

COSAIN 9 (2017) Capita Business Services Limited

Dark Justice (2017) https://darkjustice.co.uk

Derbyshire Police (2012) Guidance on the safe use of the internet and social media by police officers and police staff.

http://www.derbyshire.police.uk/Documents/About-Us/Freedom-of-Information/Policies/SafeUseoftheInternetandSocialMediabyPoliceOfficersandPoliceStaffGuidance.pdf

Digital Trends (2016). The History of Social Networking. Digital Trends. https://www.digitaltrends.com/features/the-history-of-social-networking/

Donohue, L. (2015). The Dawn of Social Intelligence (SOCINT).Georgetown University Law Center. Vol. 63. http://scholarship.law.georgetown.edu/cgi/viewcontent.cgi?article=2540&context=facpub

Echosec (2017) Echosec Systems. https://www.echosec.net/ [Accessed 1 October 2017]

Edwards, L., Urquhart, L. (2016) Privacy in public spaces: what expectations of privacy do we have in social media intelligence?. *International Journal of Law and Information Technology*, *24*(3), pp.279-310.

Haigler, K., 2012. Guide to Intelligence Support for Military Operations. *The Intelligencer Association of former Intelligence Officers*. 19(1). (pp. 51-55).

Gallagher, S., (2014). The Sad, Strange Saga of Russia's 'Sergeant Selfie'. Ars Technica. https://arstechnica.com/information-technology/2014/08/the-sad-strange-saga-of-russias-sergeant-selfie/

Gibson, S.D. (2014). Exploring the Role and Value of Open Source Intelligence. In Hobbs, C., Moran, M., Salisbury, D. (eds) *Open Source Intelligence in the Twenty-First Century* (pp. 9-23). Palgrave Macmillan UK.

Guardians of the North (2017) http://main.guardiansofthenorth.com/

Harris, M. (2017) How Peter Thiel's Secretive Data Company Pushed Into Policing. Wired. 8 September 2017. https://www.wired.com/story/how-peter-thiels-secretive-data-company-pushed-into-policing/

HMIC., (2015). Online and on the edge: Real risks in a virtual world: An inspection into how forces deal with the online sexual exploitation of children. HMIC. http://www.justiceinspectorates.gov.uk/hmicfrs/wp-content/uploads/online-and-on-the-edge.pdf

Homeland Security Research. (2017). OSINT Market & Technologies - 2017-2022. http://homelandsecurityresearch.com/OSINT-market-technologies [Accessed 1 October 2017]

Home Office (2014) Covert Human Intelligence Sources; Codes of Practice. Pursuant to section 71(4) of the Regulation of Investigatory Powers Act 2000. TSO. p.33 https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/384976/Covert_Human_Intelligence_web.pdf [Accessed 1 October 2017]

UK Home Office. (2017). Home Secretary gives £20 million boost to tackle online grooming. Press Release. Gov.uk. https://www.gov.uk/government/news/home-secretary-gives-20-million-boost-to-tackle-online-grooming

UK Home Office. (2017). Integrating the Science and Technology Support for the UK's Defence and Security. Home Office, Ministry of Defence, and Defence Science and Technology Laboratory. https://www.gov.uk/government/news/integrating-the-science-and-technology-support-for-the-uks-defence-and-security

Hunted One, The (2017) https://www.youtube.com/channel/UCA86yT9Xh_w1pVa4BadXPZQ

Hulnick, A.S., 2010. The Dilemma of Open Sources Intelligence: Is OSINT Really Intelligence?. In The Oxford handbook of national security intelligence.

ISC - Intelligence and Security Committee of Parliament., (2015). Privacy and Security: A modern and transparent legal framework. http://isc.independent.gov.uk/files/20150312_ISC_P+S+Rpt(web).pdf [Accessed 10th October 2017]

Johnson, A. H., (2016). Who's afraid of 'Russia Today'? The Nation. https://www.thenation.com/article/whos-afraid-of-russia-today/

Kent Police (1998) The JAPAN Test. https://www.kelsi.org.uk/__data/assets/pdf_file/0003/26706/Japan-Test.pdf [Accessed 1 October 2017]

Krebs, V., 2002. Uncloaking terrorist networks. First Monday, 7(4).

Kwoka, M, B., (2015). Leaking and Legitimacy. UC Davis Law Review. Vol. 48. https://lawreview.law.ucdavis.edu/issues/48/4/Articles/48-4_Kwoka.pdf [Accessed 19th October]

Lamothe, D., (2017). U.S families got fake orders to leave South Korea. Now counterintelligence is involved. Washington Post. https://www.washingtonpost.com/news/checkpoint/wp/2017/09/22/u-s-families-got-fake-orders-to-leave-south-korea-now-counterintelligence-is-involved/?utm_term=.4aee6602754e

Lesca, H., Lesca, N. (2011).Weak Signals for Strategic Intelligence: Anticipation Tool for Managers. Wiley. London, UK, ISTE. (p.32)

Lord, J. (2015) Undercover Under Threat: Cover Identity, Clandestine Activity, and Covert Action in the Digital Age, International Journal of Intelligence and CounterIntelligence, 28(4) pp. 666-69.

http://www.tandfonline.com/doi/full/10.1080/08850607.2015.1022464?src=recsys

MacAskill, E. (2015) British army creates team of Facebook warriors. 31 January 2015. https://www.theguardian.com/uk-news/2015/jan/31/british-army-facebook-warriors-77th-brigade

Mak, K., Göllner, J., Prah, P., Meurers, C., Klerx, J. (2017) Cyber Documentation and Research Center "Horizon Scanning Center" for

Cyber Analysis and Monitoring. *Handbook of Cyber-Development, Cyber-Democracy, and Cyber-Defense*, pages 1-24.

McCue, C. (2015) Data Mining and Predictive Analysis: Intelligence Gathering and Crime Analysis. Butterworth-Heinemann. (p.31)

Mercado, S.C. (2001) "FBIS Against the Axis, 1941-1945," Studies in Intelligence, Unclassified Edition 11 (pp. 33-43) https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/fall_winter_2001/article04.html [Accessed 1 October 2017]

Mercado. S. C. (2007). Sailing the Sea of OSINT in the Information Age. C*enter for the Study of Intelligence*. 48(3). https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol48no3/article05.html [Accessed 1 October 2017]

Ministry of Defence (2009) Online Engagement Guidelines. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/27933/20090805UMODOnlineEngagementGuidelinesVersion10.pdf

Ministry of Defence (2011) Joint Doctrine Publication 2-00: Understanding and Intelligence Support to Joint Operations. *Ministry of Defence Development, Concepts and Doctrine Centre*. p. 12. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/311572/20110830_jdp2_00_ed3_with_change1.pdf [Accessed 1 October 2017]

Ministry of Defence Police (2013) Ministry of Defence Police; Guidelines on the Safe Use of the internet and Social Media by MDP Officers. January 2013. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/329509/Guidelines-socialmedia-v1-jan13.pdf

Ministry of Defence. (2017). United Kingdom Security Vetting. https://www.gov.uk/guidance/security-vetting-and-clearance

National Police Chief Council (2015) NPCC Guidance on Open Source Investigation / Research. Kent and Essex Police https://www.suffolk.police.uk/sites/suffolk/files/003525-16_npcc_guidance_redacted.pdf [Accessed 1 October 2017]

NATO (2001) NATO Open Source Intelligence Handbook. http://www.oss.net/dynamaster/file_archive/030201/ca5fb66734f540fbb4f8f6ef759b258c/NATO%20OSINT%20Handbook%20v1.2%20-%20Jan%202002.pdf [Accessed 1 October 2017]

O'Sullivan, J., (2014). Russia Today is Putin's weapon of mass deception. Will it work in Britain? The Spectator. https://www.spectator.co.uk/2014/12/the-truth-about-russia-today-is-that-it-is-putins-mouthpiece/

O'Sullivan, K.T. (2017) The European Union as Guardian of Internet Privacy: The Story of Article 16 TFEU, by Hielke Hijmans. *International Journal of Law and Information Technology.*

Pattar, T., (2017). The Future of Open Source Intelligence (OSINT). DSEI Speaker Presentation. London. https://www.dsei.co.uk/dsei-strategic-conferences--seminar-programme/the-future-of-open-source-intelligence-osint#/

Perraudin, F., (2017). Paedophile hunters jeopardising police work, says senior officer. The Guardian https://www.theguardian.com/society/2017/apr/24/paedophile-hunters-jeopardising-police-work-child-protection

RepKnight (2017) RepKnight https://www.repknight.com/ [Accessed 1 October 2017]

Royal Navy (2017) Social Media. https://www.royalnavy.mod.uk/welfare/keeping-in-touch/social-media

Steele, R.D. (1995) The importance of open source intelligence to the military. *International Journal of Intelligence and Counter Intelligence*, 8(4), pp.457-470.

Sorinreq. (2017). Sorinteq Advanced Open Source Intelligence Training Course. Birmingham. January 2017. https://www.sorinteq.com/

UK Government. (1998). Human Rights Act 1998. https://www.legislation.gov.uk/ukpga/1998/42/contents [Accessed 1 October 2017]

UK Government (2000) Regulation of Investigatory Powers Act. https://www.legislation.gov.uk/ukpga/2000/23/contents [Accessed 2 October 2017]

Weiman, G., (2016). Terrorist Migration to the Dark Web. *Perspectives on Terrorism*. 10(3). http://www.terrorismanalysts.com/pt/index.php/pot/article/view/513

ELABORATION AND TESTING OF THE METHODOLOGY OF RISK ASSESSMENT AND HOME VISIT QUESTIONNAIRES FOR DWELLINGS

Kadi Luht, MSc
Estonian Academy of Security Sciences, Rescue College, Lecturer;
University of Tartu, Institute of Education, PhD student

Ants Tammepuu, PhD
Estonian Academy of Security Sciences,
Rescue College Associate Professor;
Estonian University of Life Sciences, Institute of Forestry and Rural Engineering

Helmo Käerdi, PhD
Estonian Academy of Security Sciences, Rescue College
Professor Emeritus

Tarmo Kull, MA
Estonian Academy of Security Sciences, Rescue College, Lecturer

Alar Valge, MA
Estonian Academy of Security Sciences, Rescue College, Lecturer

Keywords: fire safety of dwellings, risk assessment, home consulting methodology, testing of the questionnaire

ABSTRACT

The aim of the current study was to create a questionnaire, which provides the basis for effective assessment of fire safety conditions in homes, taking into account the possible causes and factors, which have an impact on the development and consequences of fires (including the physical and social environment of the home). The statistical data analysis was carried out to provide input for the significance of the parameters in an Estonian context in determining the weights for the index method. The list of factors which have an impact on fire safety and their corresponding assessment scales were compiled in conjunction with experts. The primary model embraces 21 parameters, which are assessed on a 5-point ordinal scale. The summary assessment is presented on a 100-point scale, with results given the following ratings: very good, good, moderate and unsafe. The home visit questionnaire was simplified during testing, according to the background and experiences of the persons carrying out the home visits and converted to be made available in Estonian Rescue Board database. The continual analysis, based in the questionnaire, generated the recorded data over nearly two thousand home visits in Estonia. For validating the questionnaire the fire safety condition of homes was mapped on the strength of different kinds of home visits (inclusive voluntary application, belonging to risk zone, after fire case) and the functionality of the questionnaire was evaluated as well.

INTRODUCTION

The number of residential fires and accompanying fatalities in Estonia is remarkably high. These fires form approximately 50% of all fires in buildings and about 80% of fires with fatalities. CTIF (Brushlinsky et al. 2017) statistic shows that the average number fire deaths per 100 000 inhabitants in 2015 was 3,8 in Estonia, quite similar to Latvia (4,4) and Lithuania (4,3) but much higher than 1,4 in Finland, 1,1 in Sweden. In 2016 this statistic was 2,97 deaths per 100 000 inhabitants in Estonia, with 92% of deaths as a result of dwelling fires. During 2016 there were 787 dwelling fires, in the years 2015 and 2014 the numbers were 790 and 991 respectively. The Estonian Rescue Board has conducted home visits since 2007, but there are almost 650 000 dwellings in Estonia and it's not possible to consult every home owner each year. Also the previously used home visit questionnaire contained a lot of data, where the factors essential to fire safety and the proportions of these were not definitely assigned. At the same time the earlier questionnaire was not designed or suitable for risk assessment. In order to raise the efficiency of home visits, the Estonian Rescue Board commissioned the Academy of Security Services to work out the methodology for the risk assessment and home visit questionnaire for dwellings (Luht et al. 2016), which this article is based on.

The aim of the study is to create a home visit questionnaire, which enables the effective assessment of fire safety in homes, taking into account the possible causes, development and factors that have an impact on the consequences of fires (including both: physical and social environment). The essential idea for measuring risk was based on causal and contributing factors from the Haddon matrix (Haddon 1972). The four columns of the Haddon matrix combine public health concepts of the host-agent-environment. The host column refers to the person at risk of injury. The agent of injury is energy (for example mechanical, thermal) that is transmitted to the host through an inanimate object or person. Environment consists of physical environments (all the characteristics of the setting in which the injury event takes place, for example a building) and social and legal norms and practices in the culture are referred to as the social environment (Haddon 1972; Runyan 1998).

Fire risk factors in the home have been described by several authors. Barillo and Goode (1996) bring out such agents as smoking behaviour,

neglected children playing with tinders, age-dependent incompetence, use of alcohol and narcotics, absence or malfunction of smoke detectors. Marshall et al. (1998) mention the roles of sex, being alone at home, age, physical or mental special needs, absence or malfunction of smoke detectors. Warda et al. (1999) mention nationality, low income, special needs, very early or late actions, type of accommodation and again smoking and use of alcohol. Leistikow et al. (2008) especially express smoking and smoking equipment as matches, cigarette-lighters etc. US Fire Administration (2002) accentuates cooking without surveillance and untended heating systems, in addition to smoking and faulty smoke detectors. Kobes et al. (2008) present multiple factors in the following four groups of characteristics: individual, social, situation specific and structured.

Some authors have specially described the characteristics, applicable for home fire risk assessment. Corcoran et al. (2011) emphasize the three main components as: building, environment and human. Higgins et al. (2013) express the significance of demographic indicators, health, poverty and disabilities, safety of neighbourhood and community sporting opportunities and dwelling features. Clare et al. (2012) introduce special subjects of home visits form the viewpoint of fire risk and safety, such as fire detector problems, evacuation plans, children and fire, fire safety concerns of the elderly and kitchens. Gielen et al. (2013) formulate the basics of home visits, which include among other things: standard of living below the poverty threshold, need for state help, racial origin of the inhabitants, ownership and age of the dwelling, etc.

Previous studies have shown that small children and aged people are at significantly increased risk in fires (Bruck 2001; Bruck et al. 2004; DiGuiseppi et al. 2002; Istre et al. 2001; Istre et al. 2002). Other important factors include; fire experience (Esmund 2000; Hooper 2004), socioeconomic status (Warda et al. 1999; Jennings 1996), living alone and special needs (Higgins et al. 2013), alcohol consumption (Jennings 1996, Warda et al. 1999) and unemployment (Warda et al. 1999). According to the results of earlier studies the main causes of fires are connected with smoking (Warda et al. 1999; Leistikow et al. 2000), children playing with matches (Heimdall Consulting Ltd 2005), problems with electricity and heating systems (Jennings 1996), untidiness in the preparation of food (Heimdall Consulting Ltd 2005).

1. COMPILATION OF RISK INDEX AND HOME CONSULTING QUESTIONNAIRE

The risk index method was used as a main risk assessment tool in the current study. The substantial principles of working out suitable methodology for the fire risk index for residential buildings were based on risk management standard ISO 31000 (2010). The index method has also been used in earlier studies for the assessment of fire safety (Hultquist and Karlsson 2000; Watts and Kaplan 2001). Similar studies have still required a different approach and thus a specific index was created for the current study.

The particular application of the Haddon matrix principles was based on the fire risk factors described in the introduction. The basic materials for the compilation of the risk index were the Estonian Rescue Board's statistics during the period 2011-2015, the data of census of people and dwellings from the database of Estonian statistics, as well as data from the database of health statistics and studies.

The questionnaire was developed further in to the applied version with the help of experts and by using Delphi method (EVS-EN 31010, 2010). The outcome of the work includes the list of essential factors of fire safety in the form of a questionnaire, which enables the assessment of the common situation of fire safety in homes with the help of a unified index of fire risk on a scale of 1 to 100, that is then divided in to three groups: "green" - very good or good, "yellow" - moderate and "red" – unsafe. The analysed results of the applied questionnaire were compared with Estonian statistics.

The risk index was compiled on the application of the Delphi method. The Delphi method is suitable for receiving trustworthy and consentaneous opinion from an expert group. The Delphi method is a structured communication method, developed as a systematic, interactive forecasting method which relies on a panel of experts (EVS-EN 31010:2010). The method is an alternative to consultation, where participants implicate each other, assuring anonymous and independent opinions of all the attracted experts (Geist, 2010). Selection of the experts presumes them to have sufficient knowledge and experience as well as good will, time and effective communication skills (Baker et al. 2013).

The expert group of 28 members was formed for the current study, taking into account the recommendations of the Estonian Rescue Board. The application of the Delphi method and the attraction of experts was conducted in three steps. During the first step the experts were forwarded a questionnaire, which embraced the parameters of the dwellings and users as the factors (21 factors) of fire outbreak and course, causes of the fires and also environmental conditions, 4 factors were removed and two added as a result of the first step. In the second step the experts were asked to evaluate the weights of 19 foregoing factors in a way that the total sum was 100 and evaluate scales on the factors. Within the third step the experts were asked to assess the arithmetic means of the weights and to make proposals to increase, leave the same or decrease these weights.

During the creation of the questionnaire the results of statistical analysis (Luht et al. 2016) found that fatality in fires was significantly more likely in the following cases: men, people living alone, everyday smokers, at least once a week alcohol consumers, retired persons, unemployed, living in the countryside and an absence of smoke detector. After transferring the completed method to the client questionnaire it was tested and analysed and proposals from Estonian Rescue Board members in different regions were proposed and changes made if needed. The final questionnaire is shown in the Appendix.

2. RESULTS AND DISCUSSION

2.1. HOME CONSULTING QUESTIONNAIRE TESTING AND ANALYSIS

The methodology of the fire safety risk assessment and home visit questionnaire were tested after compilation during the period from the 1st of May until the 7th of August 2017 in 1982 homes. The testing was carried out by a minimum two-member team of professional or voluntary rescue workers. The questionnaire was completed in the safety information system of the Estonian Rescue Board.

The conformance of the sample with Estonian generic characteristics was observed and detected, which permitted the assumption that the questions were comprehensible and fairly answered. For validating the questionnaire the differences on the risk scale were tested and the basis of home visiting by risk were compared with homes visited on another bases.

Data was analysed using SPSS (version 24.0) software. The independent-samples t-test was used to compare the differences between homes, visited on the basis of risk, with homes, visited on anohter bases Pearson's chi-square post-hoc testing based on adjusted residuals was used to compare risk and ordinary homes with a significance level $p<0,001$ and adjusted residuals >1,9.

The fire safety risk assessment testing was carried out in 1982 homes, the majority in the Western (926 consultations, i.e. 46,7 %) and Eastern (730 i.e. 36,8%) regions of Estonia. The basis of home consulting were noted information from co-partners in 209 cases (10,5%), risk area in 293 cases (14,8%) and home visits after fire in 148 cases (7,5%). On only 13 cases were the teams of home consultants not let into the dwellings.

The home fire safety situation was assessed on a 100-point scale, whereby a very good rate was received in 35,0% of homes (score < 20), good in 53,3%, (score 20-40), moderate in 10,0% (score 40-60) and unsafe in 1,6% (score > 60) of homes. The average result 26,0 (with a standard deviation

of 11,7) was in the region "good" and vastly closer to the region "very good" (20 points) than to the region "moderate" (40 points). Based on normal distribution the ranges of the risk scale could be somewhat different. Namely the very good region should be < 14 (≈ 26-11,7), good 14-26, moderate 26-38 and unsafe > 38.

Children up to 7 years old lived in 220 of the consulted homes, including two in 59 cases, three in 13 cases, four in 2 cases and five in 1 case. Children between 7 and 18 were in 347 dwellings, in 139 cases more than one (once even 6). Inhabitants between 19 and 39 years were in 546 dwellings, in 278 cases more than one. People between 40-60 years old were met in 995 dwellings, in 558 cases at least two. 65-74 year olds were in 524 dwellings and over 75 year olds in 68. In 656 dwellings (approximately one third, more precisely 32,4%) was one single resident. From 381 households with one member, the only family member was at least 65 years old. On the other hand, the number of big families was rather small: 6 to 12 inhabitants were only found in 60 consulted homes (30%).

The main language of the users of the dwellings was Estonian (61,9%). In 4,9% of the dwellings Estonian and another language were simultaneously in use, in 32,8% only Russian language and in six homes another language. According to the data from Statistics of Estonia (2017) the numbers of the represented nationalities on the 1st of January were the following: Estonians 68,76 %, Russians 25,10%, other nationalities 5,17% and persons with unknown nationality 0,97%.

Residents who were deemed to have special needs were identified in 75 of the consulted dwellings (3,8%) and in 30 cases it was hard to say. For the purpose of the question those cases deemed as hard to say were marked as having a disability. According to statistics from the Republic of Estonia Social Insurance Board (2017) approximately 10% of the inhabitants have a disability.

Alcohol non consumption or consumption only on feast days was mentioned at 75,7% of dwellings, in 22,0% of dwellings slight alcohol consumption was identified (at least four alcohol-free days per week) and 2,3% where alcohol was consumed often and in larger quantities (less than four alcohol-free days per week). This is in good accordance with the data of the Estonian Institute of Economic Research (2017), on the

grounds of which 1% of adults consumed vodka almost every day. 2% once or twice a week and 12% from one to three times weekly (85% do not drink vodka or do it rarely). About 5% of adults consumed beer almost daily, 13% once or twice a week and 23% from 1 to 3 times monthly. (59% do not drink or do it rarely).

In more than 70% of dwellings people of a working age who were employed were found and in a bit less than a fourth (22,6%) unemployed inhabitants of a working age were present, finally in 68 homes (3,3%) the answer to this question was not received. The result is in proportion with the data of Statistics Estonia, according to which in the second quarter of the year 2017 the employment rate was 66,9% and labour force participation rate 72%.

In 18,1% of visited dwellings indoor smoking was noted. This is in accordance with the results of the health behaviour study of 2016 (Health Statistics and Health Research Database (2016)), where it was found that in Estonia 21,3% of adult population are everyday smokers. Only a minor proportion of the inhabitants relate to the part of the questionnaire that embraces indoor smoking.

In most of the dwellings (59,2%) open flame devices (fireplace, gas boiler, gas stove) were absent, whereby in 23 cases (1,2%) is noted, that open flame devices were used in a hazardous way. Open flame tools (candles, matches, lighter, kerosene lamps, ethanol fireplaces) were used in hazardous way in 209 homes (10,5%).

Nearly a third (30,3%) of consulted homes had distance or electrical heating. Distance heating (boiler system) maintained by a competent person were found in 13,0% of homes. Heating devices, which were hazardous or without maintenance were identified in 56 dwellings (2,8%), in approximately half of the dwellings the heating system was maintained by competent person, which was proved by the act (33,5%) or self-maintained (20,4%).

The consultants did not notice problems with electrical installations and devices in most of the dwellings (86,1%) during primary observation. However, remarkable aging of electrical installations was found in 231 (11,7%) cases and during 44 consultations a hazardous situation was

detected when using electrical devices and installations or there was an absence of electricity in the dwelling.

Three quarters of the consulted homes (1509 homes) can solve the fire safety problems (for example connected with heating and electrical devices) by themselves. In 69 homes (3,4%) this is complicated by financial difficulties, as the problems relate to daily subsistence. In 402 cases the subsistence depends on the amount of expenditure (support is needed for a certain sum of the expenses).

Most (95,8%) of the residents of the dwellings have not experienced a case of fire in the last five years, but still 45 of the consulted persons have lived through a fire that they extinguished by themselves and in 34 dwellings where fires have happened, rescue teams were required. In four dwellings rescue teams have repeatedly been to the same address to fight fires. The entire percentage of inhabitants who have experienced a fire case was 4,2%.

Half of the dwellings (50,2%) were located in houses with a stone load bearing structure, a bit under one third (30,4) with wood and one fifth (19,5%) with a mixed structure.

57,6% of the dwellings had at least one battery powered smoke detector and in addition to the previous, 7,8% of homes had a network powered fire detecting installation. During more than one sixth of consultations, an incorrectly installed (16,9%, 334 homes) fire detection device or no fire detection device was found (17,6%, 349 homes). Thus, in a third of homes problems existed with fire detection devices or these were absent. Therefore, there is much room for significant improvement in increasing fire safety in homes.

Almost one third (32,7%) of homes had no alternative exit to the front door. In 57 homes the amount of combustible material exceeded the norm and on nine cases (0,5%) the dwellings looked like storerooms and combustible material was preventing safe evacuation and fire detection. In approximately one sixth (17,6%) of the dwellings the distribution of fire to the neighbour apartments was not impeded. The risk of fire caused by neighbours was perceived as high by inhabitants of 59 of visited homes (3,0%).

37,8% of the living dwellings were situated within five-minutes of a rescue team with a life-saving capacity. 40,1% of homes were 6-15 minutes away from a rescue team. In about one sixth of the dwellings (17,7%) the residents were aware that the arrival of the rescue team to them will take more than 15 minutes. But in 86 homes (4,3%) the inhabitants were not aware that professional help would take more than 15 minutes to reach them.

21,9% of dwellings had a primary fire extinguishing tool (extinguisher or any other) which they can use. In a few homes the fire extinguisher was not checked or was with defects during the observation (2,0%). Only in six cases the people claimed that they could not use the existing extinguisher, which shows that the main problem in that sense is hidden rather in the absence of fire extinguishers.

For analysis, results are given one of four categories: very good, good, moderate, unsafe. The particular objective was also to follow how the determined weights implicated the grouping by risk level. The four groups were compared using chi-squared post-hoc testing based on adjusted standardised residuals (> 1,9) to find out if and to what extent these groups differ from each other and the general result (Table 1, where the data are in percentages). The unsafe home group (score higher than 60 points, only 32 homes) differ from others mostly by having more disabilities, regularly using alcohol, unemployed inhabitants, smoking inside, using more open flame devices and tools, have problems with heating and electrical devices, had everyday money problems, have previously experienced fires, don't have a working fire detector, have a lot of flammable materials, there are less possibilities to hinder the spread of fire, have more dangerous neighbours and don't know that the arrival of the rescue team to them would take more than 15 minutes. The very good group (694 homes) had more only 40-64 years old inmates than general. There were not any big families in the unsafe group. Three quarters of very good homes have two to five members, almost all of them are working, don't smoke inside, don't use alcohol (or use only feast days), use open flame devices and tools safely, have safe electrical devices and fire detectors and can prevent the spread of fire.

TABLE 1. Comparison of risk and ordinary homes in percentages (in the brackets are adjusted standardised residuals)

Question	Answer variants	Risk classes				Base of home consulting		Total sample (n=1982)
		<20 points (n=694)	[20-40] points (n=1057)	(40-60] points (n=199)	>60 points (n=32)	Risk group (n=650)	Others (n=1332)	
Age of the inhabitants	19-39 years old	6,3 (2,0)	4,3 (-1,6)	3,0 (-1,3)	12,5 (2,0)	6,2 (1,7)	4,4 (-1,7)	5,0
	40-64 years old	36,7 (3,8)	26,8 (-4,6)	35,9 (1,5)	34,4 (0,4)	29,4 (-1,2)	32,2 (1,2)	31,3
	7-18 years old and/or 65-74 years old	31,6 (-1,9)	36,9 (2,5)	31,3 (-1,0)	31,3 (-0,4)	33,7 (-0,4)	34,7 (0,4)	34,4
	up to 7 years and/or over 75 years old	25,4 (-2,8)	32,0 (2,8)	29,8 (0,2)	21,9 8 (-0,9)	30,7 (0,9)	28,7 (-0,9)	29,3
Number of inhabitants altogether	2 up to 5	76,9 (8,6)	59,5 (-4,7)	47,2 (-5,3)	53,1 (-1,3)	65,7 (0,9)	63,6 (-0,9)	64,3
	6 and more	2,2 (-1,7)	3,3 (0,8)	5,0 (1,7)	0,0 (-1,0)	2,0 (-1,9)	3,5 (1,9)	3,0
	solitary	20,9 (-8,2)	37,2 (4,6)	47,7 (4,8)	46,9 (1,7)	32,3 (-0,3)	32,9 (0,3)	32,7
Spoken language of the inhabitants	Estonian	76,5 (9,8)	55,5 (-6,2)	46,7 (-4,6)	50,0 (-1,4)	54,3 (-4,9)	65,6 (4,9)	61,90
	Estonian and other (including Russian)	5,0 (0,1)	4,2 (-1,7)	7,0 (1,4)	15,6 (2,8)	5,1 (0,2)	4,9 (-0,2)	4,90
	Russian or other	18,4 (-10,2)	40,3 (7,2)	46,2 (4,1)	34,4 (0,1)	40,6 (4,9)	29,5 (-4,9)	33,10
Are there inhabitants in the living dwelling to whom special fire safety solutions have to be introduced?	NO	99,6 (7,1)	94,5 (-0,4)	81,9 (-8,5)	75,0 (-5,0)	93,8 (-1,2)	95,1 (1,2)	94,70
	YES / hard to say	0,4 (-7,1)	5,5 (0,4)	18,1 (8,5)	25,0 (5,0)	6,2 (1,2)	4,9 (-1,2)	5,30

Question	Answer variants	Risk classes				Base of home consulting		Total sample (n=1982)
What are the customs of alcohol consumption of the inhabitants?	NO consumption or only on fete days	88,5 (9,7)	74,3 (-1,6)	49,2 (-9,2)	9,4 (-8,8)	77,2 (1,1)	74,9 (-1,1)	75,70
	CONSUMED SLIGHTLY (at least four days per week without alcohol)	11,5 (-8,5)	25,2 (3,6)	40,2 (6,5)	31,3 (1,3)	18,3 (-2,8)	23,8 (2,8)	22,00
	YES, consumed often and in large quantity (less than four days without alcohol per week)	0,0 (-5,0)	0,6 (-5,5)	10,6 (8,1)	59,4 (21,6)	4,5 (4,4)	1,3 (-4,4)	2,30
Are there unemployed among inhabitants?	NO, everyone of working age is employed and earn money	94,2 (15,0)	68,9 (-5,7)	42,7 (-10,7)	6,3 (-8,8)	71,1 (-2,2)	75,6 (2,2)	74,10
	YES, there are unemployed/ hard to say	5,8 (-15,0)	31,1 (5,7)	57,3 (10,7)	93,8 (8,8)	28,9 (2,2)	24,4 (-2,2)	25,9
Is there indoor smoking (including on the balcony, window or in the basement)?	NO	98,8 (14,4)	79,8 (-2,6)	44,7 (-14,4)	15,6 8-9,8)	76,3 (-4,6)	84,7 (4,6)	81,9
	YES	1,2 (-14,4)	20,2 (2,6)	55,3 (14,4)	84,4 (9,8)	23,7 (4,6)	15,3 (-4,6)	18,1

Question	Answer variants	Risk classes				Base of home consulting		Total sample (n=1982)
Are the devices with an open flame in the dwelling used safely and are these maintained? (fireplace, gas boiler, gas stove)	YES, equipment is maintained and used safely or absent	99,7 (5,8)	97,6 (3,1)	83,4 (-10,4)	65,6 (-9,4)	94,5 (-3,3)	97,4 (3,3)	96,4
	NO, at least one unit is not maintained, but used safely	0,3 (-4,5)	1,7 (-2,2)	11,1 (8,4)	18,8 (6,1)	3,5 (2,3)	1,9 (-2,3)	2,4
	NO, equipment is used unsafely	0,0 (-3,5)	0,7 (-2,2)	5,5 (6,1)	15,6 (7,7)	2,0 (2,3)	0,8 (-2,4)	1,2
Are the tools with an open flame in the dwelling used safely? (candles, matches, lighters, kerosene lamps, etc.)	YES	96,4 (7,4)	87,9 (-2,4)	78,9 (-5,1)	56,3 (-6,2)	87,2 (-2,3)	90,5 (2,3)	89,5
	NO	3,6 (-7,4)	12,1 (2,4)	21,1 (5,1)	43,8 (6,2)	12,8 (2,3)	9,5 (-2,3)	10,5

Question	Answer variants	Risk classes				Base of home consulting		Total sample (n=1982)
Is the heating system and equipment of the dwelling maintained and safe? (oven, stove, sauna oven, fireplace)	YES, there is maintained distance or electric heating	33,9 (2,6)	29,7 (-0,6)	22,6 (-2,5)	18,8 (-1,4)	38,2 (5,3)	26,4 (-5,3)	30,3
	YES, distance heating (boiler system is maintained by a competent person)	13,1 (0,1)	14,2 (1,7)	8,0 (-2,2)	3,1 (-1,7)	12,2 (-0,8)	13,4 (0,8)	13,0
	YES, solid, gas or liquid fuel heating equipment maintained by a competent person and act exists	39,5 (4,1)	32,2 (-1,3)	22,1 (-3,6)	18,8 (-1,8)	29,1 (-2,9)	35,7 (2,9)	33,5
	YES, self-maintained but the act of the chimney sweeper is absent	13,1 (-5,9)	22,6 (2,6)	35,2 (5,5)	12,5 (-1)	16,8 (-2,8)	22,1 (2,8)	20,4
	NO, not maintained and the act of the chimney sweeper is absent and/or refers to danger (usage of heating system is inflammable)	0,4 (-4,7)	1,3 (4,3)	12,1 (8,3)	46,9 (15,2)	3,8 (1,9)	2,3 (-1,9)	2,8

Question	Answer variants	Risk classes				Base of home consulting		Total sample (n=1982)
Is the condition of dwellings electrical installations and equipment safe?	During primary observation electrical installations and equipment seem to be safe	97,4 (10,7)	88,6 (3,3)	45,2 (-17,6)	15,6 (-11,6)	85,7 (-0,4)	86,3 (0,4)	86,1
	NOT identified use of unsafe electrical equipment but still attrition if electrical equipment (plugs, electric circuit, shield)	2,4 (-9,4)	10,5 (-1,7)	44,7 (15,3)	43,8 (5,7)	11,5 (-0,1)	11,7 (0,1)	11,
	Identified use of unsafe electrical equipment and /or electrical installations are unsafe	0,1 (-4,6)	0,9 (-4,1)	10,1 (7,9)	40,6 (14,9)	2,8 (1,2)	2,0 (-1,2)	2,2
Do the inhabitants cope with making home fireproof by themselves? (for example repairing of a dangerous heating device or replacement of electrical device)	YES	91,2 (11,5)	76,3 (0,1)	35,2 (-14,3)	3,1 (-9,8)	75,5 (-0,5)	76,6 (0,5)	76,2
	DEPENDS ON THE SIZE OF THE EXPENSES (form certain sum need for help/support)	8,4 (-9,7)	22,7 (2,9)	49,2 (10,7)	18,8 (-0,2)	17,8 (-1,9)	21,5 (1,9)	20,3
	NO, problems exist also with covering of daily expenses	0,4 (-5,4)	0,9 (-6,6)	15,6 (9,8)	78,1 (23,2)	6,6 (5,3)	2,0 (-5,3)	3,5

Question	Answer variants	Risk classes				Base of home consulting		Total sample (n=1982)
Has something been on fire in the dwelling?	YES, but has been extinguished by inhabitants	1,9 (0,9)	1,7 (-1,8)	3,5 (1,2)	21,9 (7,5)	3,2 (2,0)	1,8 (-2,0)	2,3
	NO	97,3 (2,4)	96,8 (2,3)	89,4 (-4,7)	71,9 (-6,8)	92,6 (-5,0)	97,4 (5,0)	95,8
	YES, the fire was extinguished by a rescue team	0,9 (-2,1)	1,4 (-1,1)	5,5 (4,4)	6,3 (2,0)	4,0 (5,5)	0,6 (-5,5)	1,7
	YES, repeatedly (2+) fires	0,0 (-1,5)	0,1 (-1,1)	1,5 (4,3)	0,0 (-0,3)	0,1 (-0,3)	0,2 (0,3)	0,2
Which is the main building material of the dwelling?	Stone	51,6 (0,9)	49,0 (-1,1)	52,8 (0,8)	40,6 (-1,1)	52,6 (1,5)	48,9 (-1,5)	50,2
	Mixed/other	18,9 (-0,5)	20,2 (0,9)	18,6 (-0,3)	12,5 (-1,0)	18,6 (-0,7)	19,9 (0,7)	19,5
	Wood	29,5 (-0,6)	30,7 (0,4)	28,6 (-0,6)	46,9 (2,0)	28,8 (-1,1)	31,2 (1,1)	30,4
Did the smoke detector exist and was it in working order?	YES, network powered fire detection installation in working order existed	13,1 (6,4)	5,9 (-3,5)	1,0 (-3,8)	0,0 (-1,7)	10,9 (3,6)	6,3 (-3,6)	7,8
	YES, at least one battery powered smoke detector in working order existed	80,8 (15,4)	50,6 (-6,7)	23,1 (-10,4)	0,0 (-,6)	50,8 (-4,3)	61,0 (4,3)	57,6
	YES, there was, but incorrectly installed or was not in working order (battery removed) or MISSING	6,1 (-19,6)	43,5 (9,0)	75,9 (12,9)	100,0 (7,8)	38,3 (2,5)	32,7 (-2,5)	34,6

Question	Answer variants	Risk classes				Base of home consulting		Total sample (n=1982)
Does another safe exit in addition to front door exist (including window)?	YES	74,4 (4,9)	66,1 (-1,2)	49,2 (-5,7)	65,6 (-0,2)	67,2 (0,0)	67,3 (0,0)	67,3
	NO	25,6 (-4,9)	33,9 (1,2)	50,8 (5,7)	34,4 (0,2)	32,8 (0,0)	32,7 (0,0)	32,7
Is there piled dangerously much combustible materials in the dwellings and is evacuation impeded?	NO	100,0 (6,1)	97,5 (2,3)	87,9 (-7,2)	50,0 (-14,8)	93,8 (-4,9)	98,0 (4,9)	96,7
	YES, there is plenty of combustible material, but evacuation and possible detection of fire are not impeded	0,0 (-5,6)	2,4 (-1,5)	9,5 (5,9)	40,6 (12,9)	4,9 (3,8)	1,9 (-3,8)	2,9
	YES, there is plenty of combustible material and the dwelling resembles a storeroom, evacuation and possible fire detection are impeded	0,0 (-2,2)	0,1 (-2,5)	2,5 (4,6)	9,4 (7,6)	1,2 (3,6)	0,1 (-3,6)	0,5

Question	Answer variants	Risk classes				Base of home consulting		Total sample (n=1982)
Is the spread of fire to neighbouring dwellings or buildings blocked?	YES	92,4 (8,5)	82,0 (-0,5)	57,3 (-9,8)	37,5 (-6,7)	79,1 (-2,8)	84,1 (2,8)	82,4
	NO, too close to neighbouring building or non-renovated apartment house, where fire barrier doors are missing	7,6 (-8,5)	18,0 (0,5)	42,7 (9,8)	62,5 (6,7)	20,9 (2,8)	15,9 (-2,8)	17,6
Does a fire risk caused by neighbours exist?	NO	95,5 (7,9)	85,6 (-2,7)	75,4 (-5,4)	50,0 (-6,5)	81,1 (-6,0)	90,6 (6,0)	87,5
	YES, but the inhabitants consider it to be low	3,9 (-6,3)	10,8 (2,0)	20,1 (5,3)	25,0 (3,0)	14,8 (5,5)	7,0 (-5,5)	9,5
	YES, the risk from neighbours is high	0,6 (-4,6)	3,6 (1,7)	4,5 (1,4)	25,0 (7,4)	4,2 (2,2)	2,4 (-2,2)	3,0
Do the inhabitants know how far the nearest rescue team is and how fast the aid will be in reaching them? (talking about fire detection and development and calling for help)	<5 minutes away	45,7 (5,3)	36,0 (-1,9)	20,1 (-5,4)	40,6 (0,3)	33,8 (-2,6)	39,8 (2,6)	37,8
	<6-15 minutes away	36,2 (-2,6)	41,3 (1,2)	49,7 (2,9)	25,0 (-1,8)	41,2 (0,7)	39,6 (-0,7)	40,1
	>15 minutes away but the inhabitants were aware of it	15,9 (-1,6)	18,8 (1,4)	19,6 (0,7)	9,4 (-1,2)	17,2 (-0,4)	17,9 (0,4)	17,7
	>15 minutes away but the inhabitants were not aware of it	2,3 (-3,3)	3,9 (-1,1)	10,6 (4,5)	25,0 (5,8)	7,7 (5,1)	2,7 (-5,1)	4,3

Question	Answer variants	Risk classes				Base of home consulting		Total sample (n=1982)
Are there primary fire extinguishing tools, which the inhabitants can use?	YES, primary fire extinguishing tools (fire extinguisher or any other) exist and the inhabitants can use these	34,0 (9,6)	17,6 (-4,9)	6,0 (-5,7)	0,0 (-3,0)	19,1 (-2,1)	23,2 (2,1)	21,9
	YES, these tools exist but the inhabitants cannot use them properly	0,3 (-0,1)	0,3 (-0,2)	0,5 (0,5)	0,0 (-0,3)	0,5 (0,9)	0,2 (-0,9)	0,3
	YES, a fire extinguisher exists, but it has not been checked or was with defects during observation	2,2 (0,3)	2,1 (0,2)	1,5 -0,5)	0,0 (-0,8)	2,3 (0,6)	1,9 (-0,6)	2,0
	MISSING	63,5 (-9,3)	80,0 (4,7)	92,0 (5,6)	100,0 3,2)	78,2 (1,7)	74,6 (-1,7)	75,8

2.2. COMPARATIVE ANALYSIS OF RISK AND ORDINARY HOMES

To validate the questionnaire the sample was divided into two groups, depending on the basis of the home consultation. The group of at risk homes (32,7%) was formed on the basis of information received from co-partners (10,6%), risk area (14,7%) and previous fire (7,4%). The following analysis demonstrated if and to what extent at risk homes *differ* from other homes (Table 1, where the data are in percentages). The significant difference of risks in comparison to two groups was found as a result of a t-test: $t(1090) = 4,5$ ($p < 0,001$). The average risk rate of at risk homes was 2,7 points higher than the others. The score of at risk homes ($n = 650$) was in the range from 3,1 to 78,68 and the average score 27,8 (standard deviation 3,1). The score of other consulted homes was between 4,1 and 85,4 and with an average score of 25,1 and standard deviation 10,8. A score below 20 points was obtained in 31,2% of at risk homes and 36,9% other homes and below 40 points in 84,0% of at risk homes and 90,5% in other homes. A hazardous situation (over 60 points) was identified in 3,1% of the group of at risk homes and only 0,8% of other consulted homes.

The two groups were compared using chi-squared post-hoc testing based on adjusted residuals (>1,9) to find out if and to what extent these two groups differ from each other. In at risk homes there were significantly more Russian or other (non-Estonian) language speaking families than in other consulted homes. In the at risk group there are significantly more homes where problems with alcohol consumption exist, as 4,5% of at risk homes had residents who often use alcohol. In these homes remarkably more indoor smoking (23,7% vs 15,3%) was detected and in 6,6% of at risk homes there were difficulties with everyday expenses (in other homes only 2%).

Open flame devices are used in at risk homes in a more hazardous way (2% vs 0.8%), however no difference was noticed in open flame tools. Maintained distance or electric heating existed in about 40% of at risk homes and in approximately 25% of other consulted homes. Local heating equipment, maintained by a competent person was found in less than a third of at risk homes and in 35,7% of other consulted homes. Non-maintained and hazardous heating equipment was found in both

groups. In the sense of the use of hazardous electrical equipment, faulty electric equipment or absence of electricity no significant difference between groups was found.

Substantially more fires where a rescue team reacted were found in the group of at risk homes (4,0% vs 0,6%) as one basis of the formation of this group was was a previous case of fire. However, no difference between the groups was found in the cases of recurrent fires and self-extinguished fires.

Problems with fire detection devices existed in more than one third of dwellings. In the homes belonging to the at risk group more combustible materials were available (in 6,1% of these homes more combustible materials were found than the norm) and in one fifth of at risk homes problems with hindering the spread of fire. In the homes of the at risk group the hazards emanating from neighbours were considerably higher (these hazards were absent in 81,1% of the at risk group and 90,6% of other consulted homes). There were significantly more inhabitants in the families of the at risk group who were not aware of the distance of the closest professional rescue team (7,7% vs 2,7%)

CONCLUSION

A new home visit questionnaire was created as an output of the study, which takes into account the possible causes as well as development of residential fires and factors which have an impact on the consequences of these fires. The list of the essential factors of fire safety with distinctive weights was compiled and a risk index for the assessment of the fire safety situation was produced. The questionnaire has been in use since the 1st of May 2017 as a tool of home counselling, carried out by the Estonian Rescue Board.

The home visit questionnaire was tested during home consultations in 2017, whereby a very good or good rate was achieved in 88,3% of homes. 3,1% of homes belonging to the at risk group received over 60 points, thus being identified as unsafe. The answers obtained in the process of the questionnaire, which concerned alcohol consumption, smoking, working status and age of the residents, were in good accordance with the data of Statistics Estonia.

A third of homes had problems with fire detection equipment or it was absent. There is a remarkable reserve in this field to increase residential fire safety. Fire extinguishers, with the competence to use these were present in every fourth or fifth home. Among the latter, a few cases were found where a fire extinguisher was not checked or with detected shortcomings on observation. Only in six cases was it claimed that the inhabitants could not use an existing extinguisher, which demonstrates that the main problem is in the absence of the extinguisher, not the skill of using it.

Additional attention has to be turned to complementary information about the closest rescue team, because 4,3% of homes were not aware of the fact that the arrival of help could take more than 15 minutes. Fire detection equipment also needs to be emphasised more seriously. Generically we recommend to concentrate scrupulously on homes at high risk, detecting and selecting those that require supplementary help and advice.

The analysis demonstrated that belonging to the unsafe group was caused not only by the questions with big weights, but it was implicated by the

risks with smaller weights as well. The distribution into the ranges very good, good, moderate and unsafe depends on all the risks within the questionnaire, which confirms the expedient selection of the questions and weights.

ACKNOWLEDGEMENTS

In order to raise the efficiency of home visiting, the Estonian Rescue Board commissioned the Academy of Security Services to work out the methodology for a risk assessment and home visit questionnaire for dwellings, which this article is based on and the authors would like to acknowledge the Estonian Rescue Board and the Academy of Security Sciences for the opportunity to conclude and publish this article.

Contacts:

Kadi Luht
Estonian Academy of Security Sciences
Kase 61, 12012 Tallinn, Estonia
Phone: +372 696 5466
E-mail: kadi.luht@sisekaitse.ee

Ants Tammepuu
Estonian Academy of Security Sciences
Kase 61, 12012 Tallinn, Estonia
Phone: +372 696 5414,
E-mail: ants.tammepuu@sisekaitse.ee

Helmo Käerdi
Estonian Academy of Security Sciences
Kase 61, 12012 Tallinn, Estonia
Phone: +372 696 5454,
E-mail: helmo.kaerdi@sisekaitse.ee

Tarmo Kull
Estonian Academy of Security Sciences
Kase 61, 12012 Tallinn, Estonia
Phone: +372 696 5456,
E-mail: tarmo.kull@sisekaitse.ee

Alar Valge
Estonian Academy of Security Sciences
Kase 61, 12012 Tallinn, Estonia
Phone: +372 696 5460
E-mail: alar.valge@sisekaitse.ee

REFERENCES

Baker, J., Bouchlaghem, D. and Emmitt, S. (2013). Categorisation of fire safety management: Results of a Delphi Panel. *Fire Safety Journal*, 59, pp. 37-46.

Barillo, D. J. and Goode, R. (1996). Fire Fatality Study: Demographics if Fire Victims. *Burns*, 22, pp. 85-88.

Bruck, D. (2001). The Who, What, Where and Why of Waking to Fire Alarms: A Review. *Fire Safety Journal*, 36, pp. 623-639.

Brushlinsky, N., Ahrens, M., Sokolov, S. and Wagner, P. (2017). *World Fire Statistics. International Association of Fire and Rescue Services. Center of Fire Statistics*, 22. [Online] Center of Fire Statistics of CTIF. Available at: http://www.ctif.org/sites/default/files/ctif_report22_world_fire_statistics_2017.pdf [Accsessed 28 Aug. 2017].

Bruck, D., Reid, S., Kouzma, J. and Ball, M. (2004). The Effectiveness of Different Alarms in Waking Sleeping Children. In: *Human Behaviour in Fire: Proceedings of the 3rd International Symposium*. Belfast, London: Interscience Communications, pp. 279-290.

Clare, J., Garis, L., Plecas, D. and Jennings, C. (2012). Reduced frequency and severity of residential fires following delivery of fire prevention education by on-duty fire fighters: cluster randomized controlled study. *Journal of Safety Research*, 43 (2), pp. 123-128.

Corcoran, J., Higgs, G., Rohde, D. and Chhetri, P. (2011). Investigating the association between weather conditions, calendar events and socio-economic patterns with trends in fire incidence: an Australian case study. *Journal of Geographical Systems*, 13, (2), pp. 193-226.

DiGuiseppi, C., Roberts, I., Wade, A., Sculpher, M., Edwards, P., Godward, C., et al. (2002). Incidence of fires and related injuries after giving out free smoke alarms: cluster randomised controlled trial. *British Medical Journal*, 325, (7371), pp. 995-997.

Espenberg, K., Puolokainen, T. and Varblane, U. (2013). *Abikaugetes piirkondades päästeala ennetustöö, ohutusjärelevalve ning päästetöö teenuste optimaalsete osakaalude määratlemine ja sellealase planeerimismudeli väljatöötamine. Lõppraport*. [Online] Tartu: Tartu Ülikool, Tartu Ülikooli Sotsiaalteaduslike rakendusuuringute keskus RAKE. Available at: https://www.siseministeerium.ee/sites/default/files/dokumendid/Uuringud/Ennetus/2013_paasteuuringu_loppraport_final.pdf [Accsessed 28 Aug. 2017].

Estonian Institute of Economic Research, (2017). [Online]. Available at: http://www.sotsiaalministeerium.ee/sites/default/files/content-editors/Uudised_

pressiinfo/alkoholi_turg_ja_tarbimine_ettekanne.pdf [Accsessed 28 Aug. 2017].

Esmund, J, TEAM Consultants and Odgers, P. (2000). Short Report on the Community Safety Survey 2000, Fire and Emergency Services Authority (Western Australia).

Fire and fire protection in homes and public buildings: An analysis of Swedish fire statistics and fire protection strategies, A Report from the Swedish Chemicals Inspectorate, (2006). [Online]. Available at: https://www.kemi.se/global/rapporter/2006/rapport-1-06.pdf [Accsessed 28 Aug. 2017].

Geist, M. R. (2010). Using the Delphi method to engage stakeholders: A comparison of two studies. *Evaluation and Program Planning*, 33, pp. 147-154.

Gielen, A. C., Shields, W., Frattaroli, S., McDonald, E., Jones, V., Bishai, D., O'Brocki, R., Perry, E. C., Bates-Hopkins, B., Tracey, P. and Parsons, S. (2013). Enhancing fire department home visiting programs: results of a community intervention trial. *J Burn Care Res*., 34 (4), pp. e250-e256.

Haddon, W. A. (1972). Logical Framework for Categorising Highway Safety Phenomena and Activity. *Journal of Trauma*, 12 (3), pp. 193-207.

Health Statistics and Health Research Database, (2016). [Online]. Available at: http://pxweb.tai.ee/PXWeb2015/pxweb/et/05Uuringud/05Uuringud__02TKU__05Suitsetamine/TKU50.px/table/tableViewLayout2/?rxid=cd3ec702-c09a-4a7b-9a8c-c616be263251 [Accsessed 28 Aug. 2017].

Higgins, E., Taylor, M., Jones, M. and Lisboa, P. J. G. (2013). Understanding community fire risk – A spatial model for targeting fire prevention activities. *Fire Safety Journal*, 62A, pp. 20-29.

Hooper, L., Taylor, R. and Pepperdine, S. (2004). The MFB's human behaviour research Project. In: *Human Behaviour in Fire: Proceedings of the 3rd International Symposium*. Belfast, London: Interscience Communications, pp. 67-78.

Hultquist, H. and Karlsson, B. (2000). *Evaluation of a Fire Risk Index Method for Multistorey Apartment Buildings. Department of Fire Safety Engineering and Systems Safety. Report 3088.* [Online] Lund: Lund University, Department of Fire Safety Engineering. Available at: http://portal.research.lu.se/portal/files/4725595/1266574 [Accsessed 28 Aug. 2017].

Istre, G. R., McCoy, M. A., Carlin, D. K. and McClain, J. (2002). Residential Fire Related Deaths and Injuries among Children: Fireplay, Smoke Alarms, and Prevention. *Injury Prevention*, 8 (2), pp. 128-132.

Istre, G. R., McCoy, M. A., Osborn, L., Barnard, J. J. and Bolton, A. (2001). Deaths and Injuries in House Fires. *New England Journal of Medicine*, 322 (25), pp. 1911-1916.

Jennings, C. R. (1996). *Urban residential fires: An empirical analysis of building stock and socioeconomic characteristics for Memphis, Tennessee*. PhD. Cornell University.

Kalamees, T., Alev, Ü., Arumägi, E., Ilomets, S., Just, A. and Kallavus, U. (2011). *Maaelamute sisekliima, ehitusfüüsika ja energiasääst I. Uuringu I etapi lõpparuanne*. [Online] Tallinn: Tallinna Tehnikaülikool. Available at: http://vanaajamaja.ee/download/Raport.pdf [Accsessed 28 Aug. 2017].

Kalamees, T., Õiger, K., Kõiv, T-A., et al. (2009). *Eesti eluasemefondi suurpaneel-korterelamute ehitustehniline seisukord ning prognoositav eluiga. Uuringu lõppraport*. [Online] Tallinn: Tallinna Tehnikaülikool. Available at: https://www.mkm.ee/sites/default/files/suurpaneelelamute_uuringu_loppraport_trukk.pdf [Accsessed 28 Aug. 2017].

Karlsson, B. and Larsson, D. (2000). *Using a Delphi Panel for Developing a Fire Risk Index Method for Multi-storey Apartment Buildings. Report 3114*. [Online] Lund: Lund University, Department of Fire Safety Engineering. Available at: http://portal.research.lu.se/ws/files/5345108/1259310.pdf [Accsessed 28 Aug. 2017].

Kobes, M., Post, I. and Helsloot, B. de Vries. (2008). Fire risk of high-rise buildings based on human behavior in fires. In: *Conference Proceedings FSHB 2008. First International Conference on fire Safety of High-rise Buildings*. Bucharest: General Inspectorate for Emergency Situations, Bucharest Municipality, 11 p.

Leistikow, B. N., Martin, D. C. and Milano, C. E. (2000). Fire Injuries, Disasters, and Costs from Cigarettes and Cigarette lights: A Global Overview. *Preventive Medicine*, 31, pp. 91-99.

Luht, K., Käerdi, H., Tammepuu, A., Valge, A., Kull, T. and Mumma, A. (2016). *Eluruumide tuleohutuse riskihindamise metoodika ja kodukülastuse ankeedi väljatöötamine. Lõppraport*. Tallinn: Sisekaitseakadeemia.

Marshall, S. W., Runyan, C. W., Bangdiwala, S. I., Linzer, M. A., Sacks, J. J. and Butts, J. D. (1998). Fatal Residential Fires: Who Dies and Who Survives. *Journal American Medical Association*, 279 (20), pp. 1633-1637.

Risk management. Principles and guidelines. Estonian Centre for Standardisation, EVS-ISO 31000:2010.

Risk management. Risk assessment techniques. Estonian Centre for Standardisation. EVS-EN 31010:2010.

Runyan, C. W. (1998). Using the Haddon matrix: introducing the third dimension. *Injury Prevention*, 4 (4), pp. 302-307.

Social Insurance Board, (2017). [Online]. Available at: http://www.epikoda.ee/wp-content/uploads/2012/06/Ekspertiisi-statistika-1.-jaanuar-2017.xlsx [Accsessed 28 Aug. 2017].

Statistics of Estonia, (2017). [Online]. Available at: https://www.stat.ee/34278 [Accsessed 28 Aug. 2017].

US Fire Administration, (2002). Fatal Fires. Topical Research Series. 2 (20). USFA: MA.

Warda, L., Tenenbein, M. and Moffat, M. E. (1999). House Fire Injury Prevention Update. Part I. A Review of Risk Factors for Fatal and Non-Fatal House Fire Injury. *Injury Prevention*, 5, pp. 145-150.

APPENDIX

Question	Answer variants	Points	Weight
QUESTIONS CONNECTED WITH PEOPLE			
Age of the inhabitants	up to 7 years old	5	5,3
	7-18 years old	3	
	19-39 years old	0	
	40-64 years old	1	
	65-74 years old	3	
	over 75 years old	5	
Number of inhabitants altogether	1	5	3,4
	2 up to 5	0	
	6 and more	3	
Spoken language of the inhabitants	Estonian	0	2,9
	Russian	5	
	Estonian and other (including Russian)	3	
	Other	5	
	Adjustment		
Are there inhabitants in the dwellings to whom special fire safety solutions have to be introduced? (smoke detector, SMS information to people with hearing disability)	NO	0	5,4
	YES	5	
	HARD TO SAY	5	
	Adjustment		
What are the customs of alcohol consumption of the inhabitants?	NO consumption or only on fete days	0	10
	CONSUMED SLIGHTLY (at least four days per week without alcohol)	3	
	YES, consumed often and in large quantity (less than four days without alcohol per week)	5	
	Adjustment		

Question	Answer variants	Points	Weight
Are any of the inhabitants unemployed?	NO, everyone of working age is employed and earning money (including persons on maternity leave holiday and on retirement pension)	0	6
	YES, there are unemployed	5	
	HARD TO SAY	5	
	Adjustment		

QUESTIONS CONNECTED TO THE USE OF DWELLINGS

Is there indoor smoking (including on the balcony or window, in the basement)?	NO	0	10,8
	YES	5	
	Adjustment		
Are the devices with an open flame in the dwelling used safely and are these maintained? (fireplace, gas boiler, gas stove)	ABSENT	0	3,5
	YES, equipment is maintained and used safely	0	
	NO, at least one unit is not maintained, but used safely	3	
	NO, equipment is used unsafely	5	
	Adjustment		
Are the tools with an open flame in the dwelling used safely? (candles, matches, lighters, kerosene lamps, etc.)	YES	0	3,5
	NO	5	
	Adjustment		
Is the condition of the dwellings electrical installations and equipment safe?	During primary observation electrical installations and equipment seem to be safe	0	7,6
	NOT identified use of unsafe electrical equipment but still attrition if of electrical equipment (plugs, electric circuit, shield)	3	
	Identified use of unsafe electrical equipment and /or electrical installations	5	
	ELECTRICITY IS MISSING	5	
	Adjustment		

Question	Answer variants	Points	Weight
Are the heating system and equipment of the dwelling maintained and safe? (oven, stove, sauna oven, fireplace)	YES, there is maintained distance or electric heating	0	7,6
	YES, distance heating (boiler system is maintained by a competent person)	1	
	YES, solid, gas or liquid fuel heating equipment maintained by a competent person and act exists	2	
	YES, self-maintained but the act of the chimney sweeper is absent	3	
	NO, not maintained and the act of the chimney sweeper is absent and/or refers to danger (usage of heating system is inflammable)	5	
	Adjustment		
Do the inhabitants cope with making the home fireproof by themselves? (for example the repair or replacement of dangerous electrical devices)	YES	0	5,3
	DEPENDS ON THE SIZE OF THE EXPENSES (form certain sum need for help/support)	3	
	NO, problems also exist with the covering of daily expenses	5	
Has something been on fire in the dwelling?	NO	2	1,1
	YES, but has been extinguished by inhabitants	1	
	YES, has been fire where rescue team reacted	3	
	YES, repeatedly (2+) fires	5	
	Adjustment		
QUESTIONS CONNECTED TO THE ENVIRONMENT			
What is the main building material of the dwelling?	Stone	0	2,2
	Mixed/other	3	
	Wood	5	

Question	Answer variants	Points	Weight
Did the smoke detector exist and was it in working order?	YES, a network powered fire detection installation in working order existed	0	10,1
	YES, at least one battery powered smoke detector in working order existed	1	
	YES, there was, but incorrectly installed or was not in working order (battery removed)	5	
	MISSING	5	
Does another safe exit in addition to the front door exist (including window)?	YES	0	1,6
	NO	5	
	Adjustment		
Is there piled dangerously much combustible materials in the dwelling and is evacuation impeded?	NO	0	3,1
	YES, there is plenty of combustible material, but evacuation and possible detection of fire are not impeded	3	
	YES, there is plenty of combustible material and the dwelling resembles a storeroom, evacuation and possible fire detection are impeded	5	
	Adjustment		
Is the spread of fire to neighbouring dwellings or buildings blocked?	YES	0	2,1
	NO, too close to neighbouring building or non-renovated apartment house, where fire barrier doors are missing	5	
	Adjustment		
Does a fire risk caused by neighbours exist?	NO	0	4,0
	YES, but the inhabitants consider it to be low	3	
	YES, the risk from neighbours is high	5	
Do the inhabitants know how far the nearest rescue team is and how fast the aid will be in reaching them? (talking about fire detection and development and calling for help)	<5 minutes away	0	3,4
	<6-15 minutes away	3	
	>15, minutes away but the inhabitants were aware of it	4	
	>15 minutes away but the inhabitants were not aware of it	5	

Question	Answer variants	Points	Weight
Are there primary fire extinguishing tools, which the inhabitants can use?	YES, primary fire extinguishing tools (fire extinguisher or any other) exist and the inhabitants can use these	0	1,1
	YES, these tools exist but the inhabitants cannot use properly	1	
	YES, fire extinguisher exists, but it have not been checked or were with defects during observation	3	
	MISSING	5	

VERY GOOD < 20
GOOD [20 – 40]
MODERATE [40 – 60]
UNSAFE > 6

THE NATIONAL CRITICAL INFRASTRUCTURE PROTECTION PROGRAM IN POLAND – ASSUMPTIONS

Rafał Wróbel, Sr. Cpl. PhD Eng.
The Main School of Fire Service, Poland
Faculty of Civil Safety Engineering
Unit of Analysis Civil Safety
Acting Manager Department of Continuing Engineering and Decision Processes

Zuzanna Derenda
The Main School of Fire Service, Poland
Faculty of Civil Safety Engineering
Student of Internal Security

Keywords: critical infrastructure, Poland, vision of the Council of Ministers, critical infrastructure

ABSTRACT

The concept of critical infrastructure protection in Poland was defined in the National Critical Infrastructure Protection Program (NCIPP). The legal basis for its creation was provided by the provisions of the Crisis Management Act and the Ordinance of the Council of Ministers of 30 April 2010 on the National Critical Infrastructure Protection Program. NCIPP presents the vision of the Council of Ministers for the protection of key sites, facilities, installations and services in the state.

INTRODUCTION

Critical infrastructure is a special subject of protection for every country, including Poland. Critical infrastructure in Poland in accordance with applicable national law is recognised and designated. Its protection is the domain of the critical infrastructure operator and is supposed to support it in specific cases of public administration. The overall vision of the Polish State organising the protection of critical infrastructure in the form of a system was adopted in 2013 by the Council of Ministers. At present, due to the relatively short time, it is difficult to assess the effectiveness of the defined system in light of emerging threats. Bearing in mind the main research problem, the authors identified in the form of a question the following: In what scope does the critical infrastructure protection system in Poland ensure safety of critical elements of the state in light of emerging threats? In close correlation with the research problem remains the main objective of the research, which is considered as defining the assumptions of the critical infrastructure protection system in Poland. Achieving the primary research goal is possible by first implementing the specific objectives of: defining the genesis and idea of protection of critical infrastructure in Poland, identifying hazards, defining interdependencies between elements of critical infrastructure, defining formal and legal conditions for critical infrastructure protection, an indication of the general vision of the Council of Ministers regarding the protection of elements of the state considered critical, or defining the scope of actions for its protection.

It should be noted that this article fulfills a practical role expressed, inter alia, by demonstrating the critical infrastructure and identifying the threats to it, as well as the empirical role of assessing measurably the effects of the implemented critical infrastructure protection system, including measures to ensure its safety.

1. CRITICAL INFRASTRUCTURE IN POLAND

The term critical infrastructure was first used in Poland in 2002 during work carried out within the framework of NATO. It defined the critical infrastructure as "a set of essential facilities and services necessary for the proper functioning of the productive sectors of the economy (Wojciechowicz 2004)". Another working definition in the concept paper approved by the High Civil Planning Committee in December 2003 defined critical infrastructure as "buildings, services and information systems that are so important to states that their inefficiency or destruction would have a devastating effect on national security, economy, public health, public order and the effective functioning of the government (Soloch)".

A milestone in the protection of European critical infrastructure was the directive issued by the Council of Europe in December 2008 on the identification and designation of European critical infrastructure and the assessment of the need to improve its protection (Council of Europe Directive 2008/114 / EC of 8 December 2008). In view of the solutions taken at the EU level, Poland has also commenced implementation work on this issue. One of the basic issues in this matter has been the preparation of the National Critical Infrastructure Protection Program (NCIPP) defining the conditions for improving the safety of critical infrastructure.

Formal-legal determinants that encourage critical infrastructure work and its protection have been strengthened by reference to the need to protect critical infrastructure in the National Security Strategy of the Republic of Poland 2007 (National Security Bureau, 2007). The National Security Strategy of the Republic of Poland 2007 pointed to the threat to the ICT system and networks that could result from cyberspace and could imply both material losses as well as the paralysing of important spheres of public life (Ibidem). In addition, the Strategy referred to the transport infrastructure and communications, the state's telecommunications infrastructure, the banking system and, in view of the transnational dimension of the functioning of critical infrastructure, Poland's active participation in the work of its protection in NATO and the EU (Ibidem). The Act of 26 April 2007 on Crisis Management in its original version defined the critical infrastructure and its protection in a slightly different way than it is today. According to the records, critical infrastructure meant "systems

and mutually bound functional objects contained therein, including constructions, facilities, installations and services of key importance to the security of the state and its citizens as well as serving to ensure the efficient functioning of public administration authorities, institutions and enterprises" and included such systems as: energy and fuel supply; communication and telecommunications networks; financial; food and water supply; health care; transport and communication; rescue; ensuring the continuity of public administration; production, storage, curation and use of chemicals and radioactive substances, including pipelines of hazardous substances (Act of 26 April 2007).

The protection of critical infrastructure was understood by "as all steps aimed at ensuring the functionality, continuity and integrity of critical infrastructures in order to prevent threats, risks or vulnerabilities as well as limiting and neutralising their effects and the quick reconstruction of infrastructure in case of failures, attacks and other events disrupting its appropriate functioning (Ibidem)".

Recalled elements over time have been redefined and in the new form they are listed in the Act of 29 October 2010 on the amendment of the Crisis Management Act (The Act of 29 October 2010), including the definition of critical infrastructure and the updated division into systems. The systems referred to are: energy, fuel and energy resources supply systems (1); communication systems (2); tele-information network systems (3); financial systems (4); food supply systems (5); water supply systems (6); health protection systems (7); transportation systems (8); rescue systems (9); systems ensuring the continuity of public administration activities (10); systems of production, storing and use of chemical and radioactive substances, including pipelines for dangerous substances (11) (Ibidem).

Critical infrastructure protection in Poland is the domain of crisis management. Responsibility for coordinating the organisation and co-operation of critical infrastructure protection activities in Poland has been entrusted to the Governmental Center for Security, an over-the-counter structure designed to optimise and unify the perception of the threats of individual entities (Skomra, 2011) and thereby increase the ability to respond to symptoms and real and virtual threats with symmetric and asymmetric properties.

Implementing measures for effective protection of critical infrastructure in Poland is the domain of critical infrastructure operators and public administrations, including ministers responsible for critical infrastructure systems and therefore requires the involvement of public and private sector representatives in order to develop a unified approach. The adopted philosophy of collaboration enables organisations to implement the functionality, continuity, and integrity of critical infrastructure, help prevent threats, vulnerabilities or risks, and mitigate and neutralise their impact, and quickly recover the infrastructure in the event of a disaster, attacks and other events that interfere with its proper functioning. Unified methodology contributes to the promotion of public-private relations as well as increased resilience of critical infrastructures. Mutual cooperation is carried out at the strategic and operational level, in accordance with the adopted channels of information exchange.

A list of critical infrastructure facilities based on the accepted system and cross-criteria is prepared by the Director of the Governmental Center for Security in cooperation with the coordinators of the critical infrastructure systems. The criteria in question are also subject to update, which is one of the reasons for the changing number of elements in critical infrastructure systems. The number of critical infrastructure elements (critical infrastructure elements within the article mean facilities, equipment, installations and services considered critical infrastructure based on accepted IK identification criteria) within the time preriod 2012-2015, is broken down into systems and presented in Table 1.

TABLE 1. The number of critical infrastructure elements in 2012-2015 with further breakdown into systems

	1	2	3	4	5	6	7	8	9	10	11	Together
2012	186	230	60	58	1	5	2	73	20	47	0	682
2013	188	225	56	84	1	69	3	64	20	47	3	760
2014	188	162	54	85	1	67	3	63	20	44	2	689
2015	191	162	53	85	1	67	3	63	20	28	2	675

where: 1.2, (...) means the system referred to in Article 3, item 2 of the Act of 26 April 2007 on Crisis Management

Source: own elaboration based on [15], [30], [32], [42].

The majority of constructions, facilities, installations and services included in the critical infrastructure over the years have been in the energy, fuel and energy resources supply systems, and the least in the food supply system. The latter, together with the rescue system, are systems where the number of critical infrastructure elements have not changed over the years 2012-2015. In addition to assigning a specific number of critical infrastructure components to each system, there is yet another criterion for CI labeling. Its location determines the division of critical infrastructure elements into voivodships. A sample register, based on the mentioned criterion, covering the years 2013-2014, is presented in Table 2.

TABLE 2. Number of critical infrastructure elements in 2013-2014, broken down by voivodship

	Lower Silesian	Kuyavian-PPomeranian	Lublin	Lubusz	Lodzkie	Lesser Poland	Masovian	Opole	Subcarpathian	Podlachian	Pomeranian	Silesian	Świetokrzyskie	Warmian-Masurian	Greater Poland	West Pomeranian	Together
2013	50	33	31	12	28	40	242	14	36	18	46	76	17	15	59	40	757[1]
2014	45	31	28	11	24	38	221	14	34	17	41	68	15	16	47	36	686[2]

Source: own elaboration based on [32], [42].

[1] The list does not include three objects located outside the Republic of Poland.
[2] Ibidem.

2. CONDITIONS OF CRITICAL INFRASTRUCTURE SAFETY IN POLAND

Defining the determinants of critical infrastructure security in Poland is essentially a response to the key question about what elements affect its normal functioning, whereby "normal functioning" is understood to be the fulfillment of functions dedicated to this infrastructure, whether economically, public administration, entrepreneurial activity or citizen security. It is also a question of what elements of the environment should be addressed in order to answer the question of which ones may have a dysfunctional impact on the operation of critical infrastructure.

It is well-known that critical infrastructure can be dysfunctional as a result of destruction, damage or distortion of the economic development of the state, hence posing a threat to human life, health and property (Wróbel, Kulik, 2012). It is not without significance that the source of these negative events can be not only the forces of nature but also the activities of man, including intentional activity.

In addressing threats to critical infrastructure, A. Tyburska divides threats from natural forces and threats to human activity, including the abandonment of specific activities (Tyburska, 2012). In turn, W. Lidwa distinguishes three groups of threats to critical infrastructure systems and objects. These are (Lidwa et la, 2012):

- Natural hazards
- Hazards caused by human activities
- Terrorist threats to critical infrastructure

The latest approach seems to be to delineate the dangers associated with human activity, depending on whether the action is intentional (an act of terrorism) or not.

The threats of the forces of nature, in principle, does not depend on man, but are often the result of his expansive activity. The catalog of natural disasters was defined in Polish legislation in the Act of 18 April 2002 on the state of natural disaster (Act of 18 April 2002). These include (Ibidem): atmospheric discharges, seismic shocks, strong winds, intense precipitation, long-term extreme temperatures, landslides, fires, droughts, floods,

rivers and sea ice, lakes and water reservoirs, mass pests, plant or animal diseases or human infectious diseases, the action of another element.

- Man-made hazards arising from ongoing operations (exploitation) include
- Failures in industrial plants
- Uncontrolled release of large quantities of hazardous substances in transport (road, sea, rail, air, inland, pipeline, etc.)
- Collapsing buildings
- Mining shocks and accidents
- Traffic disasters (mainly rail and road)

Terrorist activities may have different backgrounds. While in most cases its primary purpose is to create fear and pressure on political groups, the causes of such activity may be many. Abstaining from the motive, terrorist activity is particularly important because of the possible effects, both physical (effects on life and health, property, environment and continuity of action) and psychological (health problems, fear of re-occurrence, psychological barrier manifesting in reluctance to invest in financial markets, etc.).

These groups of hazards should be supplemented with the possibility of critical infrastructure disruption due to its overhaul or lack of adaptability to the needs of the recipients of its services.

Among the determinants of critical infrastructure safety in Poland not only "freedom from threats" should be listed. There are also a series of conditions related to its environment, the nature of the environment, developed mechanisms of protection and maintenance of business continuity. This is as well an increase in the demand for services, networks, information systems and other critical resources. The latter are not meaningless in the context of globalisation in the area of critical infrastructure (Jakubczak, 2010) identified within corporate civilisations, whose task is to prevent or keep a crisis under control (Ibidem). Protection of critical infrastructure, already difficult in ever-changing environmental conditions, implemented through legal, organisational, continuity of action, technical and physical security, must take into account the transnational nature of critical infrastructure and the effects of its disruption or destruction. This means that it must be conducted in accordance

with clearly defined and well-known individual arrangements, rules and procedures that allow the desired protection effect to be achieved in a synergistic manner. It seems difficult, given the diversity of the involvement of individual European countries (e.g. Poland and non-European Union countries outside its structures neighboring our country) and in the first place requires the identification and designation of critical infrastructure. Difficulties in protecting critical infrastructure can also include inadequate levels of risk, and, most importantly, the unknown nature of the relationships and dependencies of critical infrastructures against each other. The effectiveness of critical infrastructure protection measures is not possible in the absence of involvement of the private sector, in most cases the critical infrastructure manager and public administration, which on the one hand guarantees the state's attention to the protection of public goods and critical assets identified as critical infrastructure, and on the other hand is also the operator of a certain number of critical infrastructures.

Critical infrastructure operators in Poland carry on their shoulders a big responsibility for the accuracy and effectiveness of their actions. These activities require constant cooperation, suitable for the needs of preparation for performing tasks and exercises of different types. Concern for critical infrastructure should be particularly prominent in the event of political involvement in international affairs and military intervention in the scene of events.

3. INTERDEPENDENCE OF CRITICAL INFRASTRUCTURE

Critical infrastructure and the network of its interrelations are complex and not fully recognised. However, it should be stressed at the outset that critical infrastructures may be dependent or interdependent. This means that the operation of one infrastructure determines the affect on another or that the infrastructures interact with one another.

By analysing the literature of the subject, one can notice that the selected authors perceive the multidimensionality of the relationship, i.e. the relations between the infrastructures. According to S. Rinaldi and J. Peerenboom, these relationships can be identified in terms of:

- Physical - the functioning of the infrastructure depends on the flow of resources from another infrastructure
- Information (virtual) - the operation of the infrastructure depends on access to information
- Geographic (geospatial) - nearly - in terms of position - the location of infrastructures in relation to one another causes them to be destroyed or disrupted as a result of a failure in one of them
- Logical (in the sense of relation) - this group forms associations not categorised in any of the existing relationships (Rinaldi, Peerenboom & Kelly, 2001)

Initially, the seen form of links was only physical and geographical (Gilette, Fisher, Peerenboom & Whitfield, 2002).

In addition to the above presented, there is another division of dependency and interdependence that allows, besides the mentioned physical, information, spatial and logical links, to identify:

- Procedural links - resulting from the rules and procedures associated with the operation of the infrastructure in question and affecting the behavior of others
- Social connections - due to the importance of infrastructure for society, which is influenced by public opinion, level of social trust, emotions or social moods, cultural and ethnic conditions (Miąsek).

Apart from the class criterion, the dependency and interdependence of critical infrastructure can be broken down according to the type, nature, type of failure that results in linkage, range, mode of operation of infrastructure, the characteristics of the couplings and reactions to them or the factors shaping the environment of the functioning of critical infrastructures (Confer Terrence). Criteria for the division of dependencies and interdependencies of critical infrastructure and linking features, depending on the criterion, are presented in Table 3.

TABLE 3. Dimensions of the dependencies and interdependencies of critical infrastructure

Division criteria		**Features of the links depending on the criterion**
Type		- Dependence - Interdependence
Class		- Physical - Cybernetic (virtual) - Geographic - Logical
Character		- Static (binding occurs continuously, regardless of system state) - Dynamic (link occurs when certain circumstances occur)
The kind of failure that a link causes		- Cascading - Common cause - Growing
Range		- Elementary - Systematic - Sector - Intersectoral
Infrastructure mode, during which dependency or interdependence manifests itself		- Normal system work - Disturbance, destruction - Restoration, regeneration
Characteristics of coupling and reaction to them	Order of dependence	- Linear - Complex
	Intensity of dependence	- Loose - Strict
	Infrastructure response	- Adaptive - Inelastic
Factors shaping the environment of infrastructures functioning		- Social/political - Health care - Safety - Technical - Legal/Regulatory - Business - Economic

Source: P. Miąsek, Dependencies and interdependencies of critical infrastructures, work on typographic rights, p. 7.

The dimensions of the dependency classification and interdependence of critical infrastructure presented in Table 3 determines both; opportunities and threats. A. Skolimowska defines these elements as a "double dimension" of the functioning of critical infrastructure: on the one hand increasing the efficiency of critical infrastructure systems by integrating their components, on the other hand increasing their susceptibility to all kinds of interference (Skolimowska, 2013). A similar approach is presented by W. Wojciechowicz, who recognises that the interconnection and dependence of critical infrastructure increases the effectiveness of its operation, but also raises the danger that any disturbance in one's functioning will adversely affect the others (Wojciechowicz, 2004). The chain character of the spread of threats, and consequently the effects of the growing disruptions in the functioning of societies, and the need to face the domino effect, which, as G. Abgarowicz suggests, would certainly lead to a weakening of the country's economic and social situation and, consequently, a decrease in the level of security and the emergence of a crisis (Abgarowicz, 2013).

4. THREATS TO CRITICAL INFRASTRUCTURE IN POLAND

Nature forces are one of the fundamental causes of critical infrastructure dysfunction. In the case of threats from their side, it is often difficult to determine the exact scope of the impact, but the expected consequences of a critical infrastructure failure make the protection tasks at all levels of government, from governmental administration to the local administration (Skomra, 2010).

In specific cases, i.e. when the constitutional forces and resources are insufficient to prevent the effects of natural disasters and technical failures, the state may exercise legal protection measures in the form of the introduction of one of the emergency states – state of natural disaster. The mode of introduction and removal of the state of natural disaster is determined by the Act of 18 April 2002 on the state of natural disaster (Act of 18 April 2002). In addition, it clarifies issues and rules of operation for the authorities and the scope of restrictions and freedoms on citizens during the time of the natural disaster. Apart from the fact that this solution is generally criticised for attributing to the state of emergency limited emergency measures (Brzeziński, 2007), since its establishment it has not yet been utilised despite the occurrence of catastrophic events and technical breakdowns.

The biggest events of this type in recent years in Poland include:

- Floods in the years 1997, 2001, 2003 and 2010
- Power shortages in a vast area covering a large group of people (Szczecin 2008, Warsaw 2012)

The biggest flood in recent years, which took place in late May and June 2010, covered 15 of Poland's 16 voivodships and resulted in many disruptions, including critical infrastructure functioning and key objects of local infrastructure (KOLI). Examples for this are:

- Energy and fuel supply systems (closed petrol stations, protection of power plants, pumping stations and fuel depots)
- Food supply system (destroying hundreds of hectares of crops in the form of orchards, fruits, vegetables and cereals)

- Financial system (need to mobilise the budget reserve)
- Rescue system (involving more than twenty thousand officers of the State Fire Brigade and over eighty thousand officers of the Voluntary Fire Brigade)
- Transport infrastructure (damaged and flooded roads and bridges)
- Communal infrastructure (closed schools, kindergartens, evacuated hospitals, flooded sewage treatment plants, damaged water supply facilities)
- Production facilities (work stopped in the glassworks, piston factory, etc.)
- Hydraulic structures (interruption or damage of flood embankments)

The scale of cascading effects for over a dozen days killed nearly thirty people, and due to its dynamic character, it required assistance from other European Union countries.

A particularly interesting case of critical infrastructure dysfunction, also triggered by heavy rainfalls of freezing rain and wet snow, wass the lack of electricity in north-western Poland (Szczecin and its surroundings) in 2008 (Pawełczyk, 2013). Its occurrence resulted in a domino effect, indicating the complexity and incomprehensible nature of the dependency of critical infrastructure. In addition, this scenario draws particular attention to - the element of time had on the primary effects.

The incident covered more than six hundred thousand people and directly affected the critical infrastructure of other systems such as:

- Energy and fuel supply systems (closed gas stations, no heating in houses)
- Communication systems (non-operation of powered telephone devices, lack of access to the Internet)
- Financial systems (inactive banks and withdrawals of cash due to ATM failures, difficulties in selling due to failures with cash registers)
- Water supply systems (non-functional water supply systems that prevent water supply)
- Health protection systems (cancelations of planned hospital operations)

- Transportation systems (trains stopped on selected cuttings due to lack of power, paused tram traffic in Szczecin) (Confer Święcka, 2010).

A noteworthy case is the blackout that occurred in December 2012 in Warsaw (Vide Owczrek, Paszcza, 2011), which was caused by damage to one of the transformers. Tens of thousands of people were without power for several hours. In addition, difficulties appeared in urban transport, supply of electricity and heat to houses. The breakdown caused a significant number of firefighting calls to people trapped in elevators, which is the primary result of similar events in the area of collective residence, mainly in middle and high-rise buildings.

A technical fault is a failure or destruction of a building or system of technical devices causing a break in their use or destruction (property loss), which has occurred in a violent and unforeseen manner. The technical failures that have taken place in Poland over recent years, resulting in a wide discussion of the causes of their emergence, include:

- Collapse of the International Katowice Fair (2005),
- Crash in the Warsaw subway (2014).

The collapse of the exhibition hall on the border between Katowice and Chorzów is the biggest catastrophe of a construction nature in recent years in Poland. As a result, sixty-five people died and several hundred were seriously injured. The cause of the collapse was a thick layer of frozen snow on the roof as well as mistakes made during construction and execution. The rescue operation lasted several days - including aid from other countries - and had a significant impact on political involvement, visible both at the scene of the action (the presence of the President, the Prime Minister, the Minister of Health and the Minister of Transport) as well as work on the amendment of the Building Law (Building Law of 7 July 1994), introducing more restrictive regulations on the safety of buildings, mainly large-area buildings.

Recalled construction failure is one of the types of technical faults that may arise for various reasons. Another type may be a malfunction in the metro caused by a sudden and uncontrolled drop in traction voltage. A tragic case was reported in July 2014 in Moscow. An analogous scenario

for the Warsaw subway is the February 2014 event, which resulted in a crash caused by a power malfunction. The irrational and uncontrolled behavior of some travelers created additional dangers. Nevertheless, due to the fact that the metro driver carried out procedure, the train crew was able to take the train to the nearest station and help deescalate the consequences of the accident.

As a result of the experience, the Subway Management Board in Warsaw decided to organise a program for social subway assistants who, as civil servants, will influence the attitude of passengers in similar situations. The metro social assistance program was launched in July 2014 and serves to improve the safety of people using the metro in unusual situations[1].

The threat of terrorism and political-military clashes is a widespread and serious phenomenon. The act of terrorism is its realisation. Regardless of its cause, the desire to induce fear, the fulfillment of missions, such events cause damage counted in the number of people killed and wounded, in property, and in the form of a decrease in confidence in ruling governments. The threat of terrorism in Poland is real. Apart from the commonly mentioned terrorist threat in the subway (Grosset, Ciekanowski, 2010), other examples of terrorist activities can be identified. The most known recent attempt to commit a terrorist attack was a case foiled by the Internal Security Agency, an attack on the Sejm of the Republic of Poland[2].

In addition to the long-standing nature of this type of activity, cyberattacks have become increasingly popular over the last few years in the area of production and exchange of information, created by communication systems. Not every incident in the network generating negative effects is directly related to cyberterrorism (soft terrorism (Leśnikowski, 2011), information terrorism or hi-tech terrorism (Confer Szubrycht, 2005)); however, due to the potential range of adverse effects on the integrity and undisturbed nature of critical infrastructure operations, NATO, the European Union and its individual member states treat this type of threat very seriously. Confirmation may be the announcement of cybersecurity strategies and programs, the search for legal protection tools

[1] http://infotram.pl/text.php?id=64946 (access: 24.07.2014).

[2] http://www.polskieradio.pl/5/3/Artykul/1034217 (access: 24.07.2014).

within the indicated scope, or the establishment of teams to respond to computer incidents. These activities are the result of the experience of countries in trying to interfere with their key systems and resources. Examples include the following:

- The attack on servers of Estonian state institutions and banks in 2007 (Confer Lichocki, 2011)
- Attack on the website of the President of Georgia in 2008
- Attacks by a worm named Stunxnet in 2010 on industrial installations
- Attack on the Chancellery of the Prime Minister of the Republic of Poland in 2012

The above examples of cyberattacks were planned and carried out by diverse, motivated groups of people and caused a range of effects. However, one can notice the common object of these attacks, information. In the sense of protecting critical infrastructure systems, it is key for the state, the entrepreneur, the corporation, and finally for society. It therefore appears that priority is given on critical infrastructure to information with a security classification.

5. THE LEGAL BASIS FOR THE CREATION OF THE NATIONAL CRITICAL INFRASTRUCTURE PROTECTION PROGRAM IN POLAND

The issue of critical infrastructure and its protection has been reflected in the provisions of the Act of 26 April 2007 (Law of 26 April 2007). It defines basic definitions for critical infrastructure protection, the purpose of creating the National Critical Infrastructure Protection Program, the principles for designating national and European critical infrastructure as well as critical infrastructure protection tasks. These tasks include:

- Collecting and processing information on critical infrastructure threats
- Developing and implementing procedures in the event of critical infrastructure threats
- Restoring critical infrastructure
- Cooperation between public administrations and owners of autonomous or dependent facilities and installations of critical infrastructure, for its protection (Ibidem).

In addition to the elements mentioned above, the Act also clarifies the obligations of critical infrastructure operators to protect their infrastructure by preparing and implementing critical infrastructure protection plans and maintaining their own backup systems to ensure the security and maintenance of the infrastructure until it is fully restored. At the same time, in implementing the requirements of the Council of Europe Directive (Council of Europe Directive 2008/114/EC of 8 December 2008), the law obliged those critical infrastructure operators to designate a person responsible for maintaining contacts with the relevant critical infrastructure protection authority.

Responsibilities for critical infrastructure operations are also defined for the Director of the Governmental Center for Security and ministers responsible for critical infrastructure systems and ministers competent for national security issues.

The abovementioned Act provides delegations with detailed solutions on how to implement obligations and co-operation within the National

Critical Infrastructure Protection Program by public administrations and national security services with critical infrastructure operators (Ordinance of the Council of Ministers of 30 April 2010), and how to create, update and structure critical infrastructure protection plans developed by operators of this infrastructure, the conditions and procedure for recognising the fulfillment of the obligation to have a plan that meets the requirements of the Critical Infrastructure Protection Plan (Ordinance of the Council of Ministers of 30 April 2010).

In addition to the listed critical infrastructure elements, the Crisis Management Act, defining the structure of crisis management plans at national, provincial, district and municipality level, indicates that they contain (Wróbel, Mytkowska, 2012):

- Hazard characteristics and risk assessment, including critical infrastructure
- Procedures for the implementation of crisis management tasks, including those related to the protection of critical infrastructure
- A list of critical infrastructure located in the voivodship, county, municipality for which a crisis management plan is being prepared
- Priorities for the protection and recovery of critical infrastructure

In addition to the Crisis Management Act and the regulations issued on 30 April 2010, the following directives on the protection of critical infrastructure include:

1. Act of 18 March 2010 on special powers of the Minister responsible for energy affairs and their execution in certain capital companies or groups operating in the electricity, oil and liquid fuels sectors (Act of 18 March 2010),
2. Ordinance of the Council of Ministers of 3 December 2015 on the Government Plenipotentiary for Strategic Energy Infrastructure (Ordinance of the Council of Ministers of 3 December 2015).

6. NATIONAL CRITICAL INFRASTRUCTURE PROTECTION CONCEPT

The National Critical Infrastructure Protection Program is a doctrinal document in the field of critical infrastructure protection in Poland, which creates conditions for its improvement by preventing disturbances in its operation, crisis preparedness transferring critical infrastructure impact, responding to disruptions or destruction and its recovery (Vide Kowalczyk, 2012).

Coordination of its preparation, the legislator ceded the Director of the Government Security Center, although the process of its preparation was based on the cooperation of the Governmental Center for Security with the ministers-coordinators of critical infrastructure systems. The preparation of the National Critical Infrastructure Protection Program is a multi-stage work involving multilateral consultations, both on the definition of criteria to distinguish critical infrastructure within its systems as well as the ready-made project of the National Critical Infrastructure Protection Program.

The program identifies national priorities, objectives, requirements and standards to ensure the effective functioning of critical infrastructure and detailed sectoral and cross-sectoral criteria in the form of numerical thresholds to distinguish facilities, installations, equipment and services included in critical infrastructure systems, taking into account their importance for the functioning of the state and the needs of citizens. The program identifies the bodies and entities implementing its objectives, primarily the role of the Governmental Center for Security, critical infrastructure operators and ministry hosts (coordinators) of the systems, their tasks, and responsibilities in the process of improving critical infrastructure protection. The manner of the realisation of duties and cooperation within the scope of the National Critical Infrastructure Protection Program is laid down in the Ordinance of the Council of Ministers of 30 April 2010.

The National Critical Infrastructure Protection Program integrates the elements previously provided for in the National and Voivodship Critical Infrastructure Protection Plans.

The methodology of its preparation was based on the will and the need to maintain good relations between stakeholders. Participation in co-operative work to improve critical infrastructure security is based on cooperation, mutual trust and sharing of responsibility. These principles contribute to the strengthening of public-private partnerships through conferences, seminars, forums for information exchange, preparation and participation in exercises and training.

The National Critical Infrastructure Protection Program was adopted by the Council of Ministers by way of a resolution. It is also updated - at least once every two years, on the initiative of the Director of the Governmental Center for Security or at the request of the competent minister-coordinator of the critical infrastructure system. Voivodes and operators of critical infrastructure may also apply for changes in it.

7. MEASURES TO ENSURE THE SAFETY OF CRITICAL INFRASTRUCTURE

The National Critical Infrastructure Protection Program defines the scope of activities undertaken by the stakeholders of the program. Their contemporary character differs slightly from the actions to protect the critical infrastructure defined in the original concept. They include organisational and technical activities, as well as educational activities aimed at providing physical, technical, personal, ICT and legal security for critical infrastructure components and for maintaining and restoring CI functions.

The National Critical Infrastructure Protection Program for the years 2015-2017 contains a clearly defined organisational, legal, technical, educational and training plan.

The need for continuous education in the light of emerging challenges and dangers cannot be surprising and becomes something completely understandable. It fits perfectly into the concept of protection as a process and is something that is continuous and repetitive.

Education and the organisation of exercises are essential to improve critical infrastructure operators' skills and ability to respond to emergencies. On the other hand, due to the fact that public administration also has critical infrastructure and coordinates the intervention and corrective actions taken as a result of critical infrastructure dysfunction, it is interested in raising awareness and knowledge about critical infrastructure and its protection.

Special tasks in the field of educational activities in the process of critical infrastructure protection are:

- Ministers responsible for critical infrastructure systems - promoting educational programs at the system level and engaged in the preparation and dissemination of strategies that encourage the private sector to participate in the National Critical Infrastructure Protection Program

- Governmental Center for Security - most interested in promoting educational programs and activities to raise public awareness of the dangers and forms of critical infrastructure protection

Education, its popularisation and training in critical infrastructure protection are implemented by all parties involved in the process of critical infrastructure protection in a variety of areas.

Admittedly, in the strategic document, the National Critical Infrastructure Protection Program, education and training activities have been separated from the mechanism of ongoing information exchange and the organisation of critical infrastructure protection forums, nevertheless, participation in these projects is inextricably linked to the possibility of gaining experience, acquiring knowledge of new solutions, legal interpretations and working in expert teams. In the area of training, counseling and conferences, a particularly desirable and valuable initiative is the latter, on the one hand, to exchange information between critical infrastructure operators, public administrations and the science world, and on the other hand, the opportunity to popularise critical infrastructure issues, ask questions and respond by meeting parties.

CONCLUSIONS

Critical infrastructure and its protection in Poland are part of a broader European Union strategy focused on recognised and identified potentially European critical infrastructure. The first steps in the implementation of the 2011 directive have resulted in the form of the provisions of the Crisis Management Act.

Critical infrastructure protection in Poland is based on critical infrastructure operators, but public administration interested in critical infrastructure security support a specific range of private sector operations.

The problem of research in the article "What is the scope of the critical infrastructure protection system in Poland ensuring the safety of critical elements of the state in the light of emerging threats?" was resolved. This was possible thanks to the goal of the main research (defining the assumptions of the critical infrastructure protection system in Poland) and the specific objectives.

This article aggregates critical infrastructure protection requirements arising from potential and emerging threats to critical infrastructure, its dependencies and its efforts to improve its security.

The content presented for private sector practitioners, on the one hand shows the dependencies between the different elements of critical infrastructure and identifies threats to it, and on the other hand empirically validates the assumptions of the implemented critical infrastructure protection system, including measures to ensure its safety, physical, technical, personal, teleinformatic, legal and reconstruction plans.

Obtaining answers to problems and thus achieving objectives is possible using two-way methods, both theoretical and empirical. In the preparation of the paper the authors used research methods such as analysis, synthesis, abstraction, comparison, generalisation, classification, interview and observation. Analysis (elementary, conceptual, qualitative, functional, comparative, systematic, etc.) allows for individual consideration of elements and consists of examining individual events, states or functions. Thanks to the synthesis, it is possible to take a comprehensive look at the cooperation of critical infrastructure protection organisations

in Poland. Methods such as interview and observation were used in the context of collecting quantitative data on the critical infrastructure in each system, identifying threats to critical infrastructure and defining their interdependencies.

Applied research methods are divided into theoretical and empirical. The most important are: analysis, synthesis, abstraction, comparison, generalisation, classification, interview and observation. Each of the described methods has been applied in particular elements of the study, e.g. analysis (elementary, conceptual, qualitative, functional, comparative, systemic, etc.) in the analysis of elements and in examining individual events, states or functions, while synthesis generated a comprehensive view on the interaction of entities and protection of critical infrastructure in Poland.

Contacts:

Rafał Wróbel
The Main School of Fire Service
Faculty of Civil Safety Engineering
Unit of Analysis Civil Safety
E-mail: rafalwrobel.sgsp@gmail.com

Zuzanna Derenda
The Main School of Fire Service
Faculty of Civil Safety Engineering
E-mail: zuzanna.derenda@gmail.com

REFERENCES AND SOURCES

Abgarowicz G., Critical Infrastructure, lecture for PhD students of the National Security Department of the National Defense Academy (March 2013).

Act of 18 April 2002 on the state of natural disaster (Journal of Laws of 2002, No. 62, item 558).

Act of 26 April 2007 on Crisis Management (Journal of Laws of 2007, No. 89, item 590; From 2013 pos. 1166; From 2015 pos. 1485).

Act of 18 March 2010 on special powers of the Minister responsible for the energy affairs and their execution in certain capital companies or groups operating in the electricity, oil and liquid fuels sectors (Journal of Laws of 2010 no. 65, item 404).

Act of 29 October 2010 on amending the Crisis Management Act (Journal of Laws of 2010 No. 240, item 1600).

Brzeziński M., Extraordinary States in Polish Constitutions, Sejm Publishing House, Warsaw 2007.

Building Law of 7 July 1994 (Journal of Laws of 1994 No. 89, as amended 414).

Council of Europe Directive 2008/114 / EC of 8 December 2008 on the identification and designation of European Critical Infrastructure and the assessment of the need to improve its protection (Journal of Laws UE, L 345, 23/12/2008 P. 0075-0082).

Gillette J., Fisher R., Peerenboom J., Whitfield R., Analyzing Water/ Wastewater Infrastructure Interdependencies, Infrastructure Assurance Center, p. 2, http://www.dis.anl.gov/pubs/42598.pdf (access: 15.06.2013).

Grosset R., Ciekanowski Z., Critical infrastructure threats on an example of the Warsaw subway [in:] Tyburska A. (ed.), Critical Infrastructure Protection, Pub. WSPol, Szczytno 2010.

http://www.infotram.pl/text.php?id=64946 (access: 24.07.2014).

http://www.polskieradio.pl/5/3/Artykul/1034217 (access: 24.07.2014)

Jakubczak W., Globalization and Critical Infrastructure [in:] Tyburska A. (ed.), Critical Infrastructure Protection, Pub. WSPol, Szczytno 2010.

Kowalczyk E., Functional analysis of the National Critical Infrastructure Protection Program, Engineering Thesis, Defended at SGSP, Warsaw 2012.

Kulik I., Security of European Critical Infrastructure Facilities in maritime areas [in:] Kustra W. (ed.), Armed Forces Cooperation with Public Administration in maritime areas, Pub. SRWO, Warsaw 2012.

Leśnikowski W., Cyberattacks on critical infrastructure as cheap and effective means of paralyzing developed states, "Review of the Air Force", 2011, No. 4 and 5.

Lichocki E., Cyberterrorism as a new form of security threat [in:] Liedel K. (ed.) Trans-sectoral areas of national security, Pub. Difin, Warsaw 2011.

Lidwa W. et al., Critical Infrastructure Protection, Pub. AON, Warsaw 2012.

Miąsek P., Dependencies and interdependencies of critical infrastructures, work on typographic rights.

National Security Bureau, National Security Strategy of the Republic of Poland 2007.

Owczarek L., Paszcza M., Crisis management in local government, Pub. Municipium, Warsaw 2011.

Pawełczyk M., Case study: Power supply failure in West Pomeranian Voivodeship from 8 to 14 April 2008 [in:] Pawełczyk M., Public-legal obligations of energy companies as an instrument for ensuring energy security in Poland, Pub. Adam Marszałek, Toruń 2013.

Rinaldi S., Peerenboom J., Kelly T., Identifying, Understanding and Analyzing Critical Infrastructure Independence, IEEE Control Systems Magazine, December 2001.

Ordinance of the Council of Ministers of 30 April 2010 on the National Critical Infrastructure Protection Program (Journal of Laws of 2010 No. 83, item 541).

Ordinance of the Council of Ministers of 30 April 2010 on Critical Infrastructure Protection Plans (Journal of Laws of 2010 No. 83 item 542).

Ordinance of the Council of Ministers of 3 December 2015 on the Government Plenipotentiary for Strategic Energy Infrastructure (Journal of Laws of 2015, item 2116).

Skolimowska A., Interdependencies of Critical Infrastructure [in:] Wróbel R. (ed.), Critical Infrastructure Protection System, Warsaw 2013.Socha R., Extraordinary States in the State, "Defense Knowledge", 2010, No. 4 (235).

Skomra W., Crisis management - a practical guide to the amendment of the Act, Pub. Presscom, Wrocław 2010.

Skomra W., Contemporary threats - challenges of the changing internal security environment [in:] Sobolewski G., Majchrzak D. (ed.), Crisis management in the national security system, Pub. AON, Warsaw 2011.

Skomra W., Materials from the speech on "Cooperation between the administration and the private sector in the area of business continuity", 1st National Congress of Business Continuity Management, Jachranka (26-27 March 2015).

Soloch P., NATO and Critical Infrastructure Protection, http://www.bbn.gov.pl/dokumenty/NATO_a_ochrona_infrastruktury_krytycznej.pdf (access: 7.07.2008).

Szewczyk T., Materials from the speech on "National Critical Infrastructure Protection Program - past experience", Conference "Ensuring continuity of functioning of state organs in the face of present threats", Szczytno (23-24 September 2014).

Szubrycht T., Cybercrime as a new form of terrorist threat, "Scientific Journal of the Naval Academy" 2005, No. 1 (160).

Święcka A., Energy security of the state as a factor of energy security, "Polish Knowledge Management Association. Series: Studies and Materials" 2010, No. 33.

Terry Terrence K., Infrastructure Interdependencies, White House Office of Science and Technology Policy, http://wpweb2.tepper.cmu.edu/ceic/presentations/Kelly.pdf (access: 15.12.2013).

Tyburska A., Critical Infrastructure Protection. Outline of issues, Pub. WSPol, Szczytno 2012.

Wojciechowicz W., Critical Infrastructure Protection of the State, "Military Thought" 2004, No 1.

Wróbel R., Kulik I., The Role of Public Administration in Critical Infrastructure Protection [in:] Piątek Z., Olearczyk S. (ed.), Defense preparation in the activities of government administration, Pub. Association of the Movement of the Defense Communities, Warsaw 2012.

Wróbel R., Mytkowska M., "Critical Infrastructure Protection and the obligation to develop plans and programs under the crisis management act", AON Doctorate Books 2012, No. 2.

Wróbel R., Kulik I., Decision Making in Critical Infrastructure Protection Organizations [in:] Piątek Z., Truchan J. (ed.), Critical Infrastructure Protection Technologies – External European Union, Pub. Association of the Movement of the Defense Communities, Szczytno 2013.

Wróbel R., Preparation of Critical Infrastructure Protection Organizations in Poland, Pub. SGSP, Warsaw 2016.

Wróbel R., Derenda Z., The concept of critical infrastructure protection in Poland for years 2015-2017, "Vedelem Tudomany".

BELIEF IN SUPERSTITION AND LOCUS OF CONTROL AMONG PAID AND VOLUNTEER RESCUE WORKERS

Kristjan Kask, PhD
Tallinn University, School of Natural Sciences and Health
Associate Professor of General Psychology

Keywords: belief in superstition, locus of control, rescue workers, volunteers

ABSTRACT

Belief in superstition is common in our society and can create an illusory feeling that a person has control over the uncertain. This study aims to examine more closely the relation of belief in superstition and locus of control among Estonian rescue workers. It is of interest whether and which superstitious items and activities the rescue workers use. It is proposed that locus of control is positively associated with belief in superstition. Also differences between paid and voluteer rescue workers are examined. One hundred rescue workers filled in a questionnaire including Rotter's (1966) locus of control scale and Fluke et al.,'s (2014) belief in superstition scale. It was found that locus of control and belief in superstition were positively associated. Those rescue workers who mentioned at least one item also scored higher in both scales. However, there were no differences between professional and volunteer rescue workers.

1. INTRODUCTION

1.1 BELIEF IN SUPERSTITION

Belief in superstition is common in our society (Matute, Yarritu & Vadillo 2011; Vyse 2000), for example that knocking on wood keeps the bad away or certain items bring good luck or help in avoiding bad luck. Fluke, Webster and Saucier (2014) claim that belief in superstition as a rule is harmless, but can lead to irrational decisions (see also Matute, Yarritu & Vadillo 2011).

In common knowledge, belief in superstition is a broad definition, starting from believing in supernatural power to certain omens (Rudski 2004). Previous research has narrowed the definition, for example Fluke et al. (2014) define superstitious beliefs as a perceived causal relationship between the behaviour and the result in a situation where there is no causal relationship present, e.g. beliefs in good and bad luck (see also Carlson, Mowen & Fang 2009; Matute, Yarritu & Vadillo 2011). Believing in good and bad luck is a factor which influences human behaviour and can be domain specific (e.g., seen in weddings, gambling, sport or health, see Jahoda 1969). Also, belief in superstition has been found to be linked to other constructs, for example Sachs (2004) noted among Chinese students that when self-efficacy was lower then the level of belief in superstition was higher.

Belief in superstition is related to cultural norms and thus differs between certain areas (Simmons & Schindler 2003). In their study in China it was found that prices ending with the digit 8 are common as there is a belief that the number 8 brings luck, prosperity, and happiness, whereas prices ending with the digit 4 are less prevalent as this number is believed to bring bad luck. Hence, it is no surprise that the Beijing Summer Olympic games were scheduled to be opened on August 8 2008 at 8 PM. In another study it was noted that people may not want to go to their workplaces on Friday the 13th so the economy may also suffer (based on Kramer & Block 2008, in the US, up to 900 million dollars for each such Friday).

Thus, belief in superstition can create an illusory feeling that a person has control over the uncertain (Matute 1994). Superstition can appear in a larger magnitude in situations with increased uncertainty and stress (such as sports events, gambling and activities related to highened risks). A way of coping with the uncertainty can be believing in superstition (Matute 1994) to gain control over the situation. Previous research has shown that superstitious behaviours can increase with the uncertainty of a situation (Rudski, Lischner, & Albert 1999). Campbell (1996) argues that belief in superstition is somewhat paradoxical as on one hand our modern society strongly believes in science and rational thinking. However, if a person starts to practice superstition in uncertain situations to gain (illusory) control over the situation, then society's belief in rationality is violated. Thus, superstitious beliefs can be related to individuals' perceived control over the environment.

1.2 LOCUS OF CONTROL

According to Rotter (1966), people who believe that the events taking place in their life are based on their behaviours, personality characteristics and efforts have internal locus of control, whereas those who think that events in their lives are based on luck, circumstances, the will of god, have an external locus of control. Thus, people with internal locus of control can believe that achieving the result is controllabe and related to the environment, however, those with external locus of control believe that the world is not controllabe, but guided by some external features. Previous research has found that those who have internal locus of control, achieve more in school and work, act more independently and feel less depressed than the 'externals' (Lefcourt 1982; Ng et al. 2006). Similar findings have also been found in long-term studies (Gale et al. 2008) and also in different samples such as mineworkers (Sims, Graves & Simpson 1984). There is also a positive relationship between external locus of control and beliefs in superstition (see Fluke et al. 2014) and this relationship has also been examined in adolescents (Sagone & De Caroli 2014) and in athletes (Todd & Brown 2003; Burke et al. 2006).

However, Fluke et al. (2014) claim that these behaviours related to sports are rituals and thus not the same as beliefs in superstition because an athlete may not necessarily believe that only the ritual has an effect on his/her performance. Still, individuals who wish in a larger extent to control the situation demonstrate higher levels in believing superstition in stressful situations (Keinan 2002) and may also believe that superstition helps them to achieve their goals. Thus, we have several confirmations that a need for control (Burger & Cooper 1979) is related to larger superstitious beliefs (see also, Darke & Freedman 1997).

1.2.1. Rescue workers, belief in superstition and locus of control

Now, imagine a situation where a fire rescue team is on their way to the site and one of the rescue workers discovers that his/her necklace that brings good luck has gone missing. The team arrives to the scene and every member of the team starts to work based on their role in the team, but all the one team member can think of is his/her missing necklace and what bad luck this could bring to him/her and the team. Suppose nothing major happens but if it does then the rescue worker's beliefs are confirmed, so if he/she does not find the necklace before the team's next call then it can continue to influece the work.

In Estonia, every day nearly 350 rescue workers are ready to react in the professional rescue system, divided between 72 commandos and 1695 workers in total (Päästeamet 2017). Besides the professionals, the rescue system also relies on volunteer rescue workers. There are over a hundred volunteer commandos in Estonia with over 1700 volunteers (Päästeamet 2017). It is known that rescue workers face unexpected situations in their daily routine and are at increased risk of stress reactions (including post-traumatical stress disorder), which can affect both their physical and mental health, and decrease their performance (see Berger et al. 2011). Thus, it is of interest how the rescue workers cope with these situations.

Previous research has indicated differences between paid workers and voluteers. For example, Elshaug and Metzer (2001) found differences between paid food preparers and volunteer food preparers and volunteer firefighters, namely voluteers were more agreeable and extraverted. Lee and Olshfski (2002) noted that paid firefighters were higher on their

commitment to their supervisor, while volunteers were higher on commitment to the organisation.

1.3 AIMS OF THE STUDY

This study aims to examine more closely the relation of belief in superstition and locus of control among Estonian rescue workers. Previous research has also found that people use either behaviours or charms to bring good luck or keep bad luck away (Fluke et al. 2014). Thus, belief in superstition is operationalised in present research as beliefs in good and bad luck.

These constructs have been examined previously in several samples (see Fluke et al. 2014; Sagone & De Caroli 2014; Todd & Brown 2003; Burke et al. 2006) but these issues are not examined in terms of rescue workers. It is proposed that external locus of control is positively associated with belief in superstition.

Some research has found that superstition is negatively associated to self-efficacy (Tobacyk & Shrader 1991) whereas another has noted improvement in performance (Damisch, Stoberock, & Mussweiler 2010). Therefore, it is also of interest whether and which superstitious items the rescue workers use and how these are related to the belief in superstition and locus of control.

Finally, as the differences in locus of control and believing in superstition have not been examined previously in paid and voluteer rescue workers then this notion is examined more closely.

2. METHOD

2.1. SAMPLE

One hundred rescue workers (mean age 34.12, SD = 3.14; 98 men) filled in the questionnaire the pen-and-pencil method, 50 paid (all men) and 50 volunteers (two women). 83 respondents considered their native language Estonian and 17 Russian. Mean work experience among the paid workers was 11.84 years (SD = 7.67, range 1-30 years) and volunteers 10.66 years (SD = 9.88, range 1-51 years).

2.2 INSTRUMENTS

The Belief in Superstition Scale (BSS, Fluke et al. 2014) was used to measure belief in superstition and the Locus of Control scale (LOC, Rotter 1966) was used to measure locus of control. The instrument consisted in total of 46 items.

First, three open-ended questions were created to examine the items rescue workers may use in their work (name items that bring you luck; name your commando items that bring you luck; and name the items of your commando technical equipment that bring you luck). The respondents could answer the questions or leave them blank. These answers were coded later to categories using qualitative content analysis (Laherand, 2008). Based on the content analysis the following three categories were formed, 1) jewellery (i.e. cross), 2) items (i.e. crystals), and 3) symbols (i.e. numbers). The answers were coded independently by two coders. The codes were compared and differences were solved during the discussion. The inter-coder reliability was Cohen's kappa $k = 0.95$ ($p < 0.001$).

LOC consists of 29 paired items (Rotter, 1966). In each of the item pairs, one is worded internally and the other externally. The respondent has to choose each of the pairs of items which he/she prefers. Six items are fillers and not taken into account in the final result. The scale is coded in a way that the higher the score the stronger the external locus of control is.

The internal consistency of the scale is Cronbach's alpha α = 0,65 - 0,79 (M = 5.48 .. 10.00, SD = 2.78 .. 4.20, Rotter, 1966). In the Estonian version of LOC the internal consistency was found to be Cronbach's alpha α = 0.67 (Sild, 2004). Examples of paired items are: 'The average citizen can have an influence in government decisions' or 'This world is run by the few people in power, and there is not much the little guy can do about it'.

BSS consists of nine items (Fluke et al. 2014) that form three factors: belief in good luck (Cronbach's alpha α = 0,68, M = 3.26, SD = 1.80); belief in bad luck (Cronbach's alpha α = 0.75, M = 4.21, SD = 1.88) and belief in change of luck (Cronbach's alpha α = 0.65, M = 3.75, SD = 1.84). The respondent had to answer items in a nine-point Likert scale (1 – strongly disagree to 9 – strongly agree). The higher the score, the more a respondent believes in supersitition. One statement is coded reversely. Examples of items are presented in Appendix A.

APPENDIX A

Items in EST	Original items in ENG	Back-translation from EST into ENG
Reede 13 on ebaõnne toov päev	Friday the 13th is unlucky	Friday 13th brings bad luck
Kui palutakse valida number, siis ma valin oma õnnenumbri	When asked to choose a number I tend to go with a lucky one number	If I'm asked to pick a number, then I'll pick my lucky number

Note: Two items of the scale are provided.

The procedure of DeVellis (2003) was used to translate BSS into the Estonian language. The items were translated into Estonian by two persons. An expert group consisting of three persons compared the translations and a final set of items were selected. The items were translated back into English by one person and compared to the original items. If necessary, then corrections were made (see Appendix A).

Finally questions about respondents gender, age, native language, status (paid or volunteer rescue workers) and average work experience were asked.

3. RESULTS

In Table 1 are presented the numbers and proportions of answers to open-ended questions for the items used. As can be seen, a large proportion of the participants did not mention any of the superstitious items.

Next, the differences between paid and voluteer rescue workers concerning answers to the statements about the items was analysed using chi-square analysis in Fisher's Exact method (see Table 2). As one participant could mention several items then the proportions of the 'did not answer' differs between Tables 1 and 2. Overall, there were no statistically significant differences between paid and volunteer rescue workers present in the usage of items.

TABLE 1. The distrtibution of answers of paid and volunteer rescue workers to the open-ended questions

Statement	Paid		Volunteer	
	Did not respond	Responded	Did not respond	Responded
Personal items that bring luck	37 (74%)	13 (26%)	39 (78%)	11 (22%)
Commando items that bring luck	42 (84%)	8 (16%)	44 (88%)	6 (12%)
Techiqal equipment items in commando that bring luck	46 (92%)	4 (8%)	47 (94%)	3 (6%)

TABLE 2. The distribution of answers concerning items of paid and volunteer rescue workers to the open-ended questions

Statement	Group	Did not answer	Jewellery	Items	Symbols
Personal items that bring luck	Paid	32 (64%)	8 (16%)	8 (16%)	2 (4%)
	Volunteer	37 (74%)	6 (12%)	5 (10%)	2 (4%)
Commando items that bring luck	Paid	38 (76%)	-	12 (24%)	0 (0%)
	Volunteer	42 (84%)	-	7 (14%)	1 (2%)

Statement	Group	Did not answer	Jewellery	Items	Symbols
Techiqal equipment items in commando that bring luck	Paid	46 (92%)	4 (8%)	-	0 (0%)
	Volunteer	47 (94%)	1 (2%)	-	2 (4%)

Now the data about BSS is presented. The Kaiser-Meyer-Olkin's index KMO = .815 ($p < .001$) indicated that the sample was large and had enough power to conduct exploratory factor analysis. Next, principal component analysis with varimax rotation (communalities and factor loadings) and reliability (if item deleted) analysis was performed. The first analysis was done using all items. Principal component analysis (EIGN ≥ 1) showed a three-component solution which explained 65.48% of the variance of data. One factor consisted of four items (two bad luck and two change luck, loadings between .65 - .84), the second factor consisted of four items (three good luck and one bad luck, loadings .49 - .90), and the third factor consisted of one item (change luck, loading .89). The first two factors were correlated (Pearson), $r = .56$; $p < 0.01$ but the third factor was not correlated with any of the first two factors.

Thus, the item from the third factor was removed and another principal component analysis was performed with eight items where the number of eigenvalues was set to two. Principal component analysis now showed a two-component solution that explained 59.69% of the variance of data. The first factor, labelled bad and changing luck, consisted of four items (two bad luck and two change luck, loadings between .65 - .84, M = 14.61, SD = 7.30, range 4 - 33, Cronbach's alpha $\alpha = .754$), the second factor labelled good luck, consisted of four items (three good luck and one bad luck, loadings .54 - .89, M = 12.47, SD = 7.80, range 4 to 34, Cronbach's alpha $\alpha = .738$).

Now the association between LOC and BSS subscales are analysed. The mean score in LOC was M=10.50, SD=3.39, range 2-21, Cronbach's alpha $\alpha = .610$. LOC and BSS subscale belief in good luck were positively correlated (Pearson), $r = .276$, $p < .01$ and LOC and BSS subscale belief in

bad and changing luck were also positively correlated (Pearson), $r = .202$, $p < .05$.

Next, it was examined whether mentioning items in the first part of questionnaire was related to LOC and BSS subscales using independent samples t-tests. Those rescue workers who mentioned at least one item that brings them luck scored higher (i.e. had more external locus of control) in LOC scale, $t(98) = -2.17$, $p < .05$ ($M = 10.10$, $SD = 3.16$ vs $M = 11.79$, $SD = 3.82$), in the BSS bad and changing luck scale (i.e., believed more in superstition), $t(98) = -3.31$, $p < .001$ ($M = 13.32$, $SD = 6.70$ vs $M = 18.70$, $SD = 7.73$) and in the BSS good luck scale, $t(98) = -7.81$, $p < .001$ ($M = 9.91$, $SD = 6.06$ vs $M = 20.58$, $SD = 7.23$). Those rescue workers who mentioned at least one commando item that brings them luck scored higher in the BSS good luck scale, $t(98) = -2.52$, $p < .05$ ($M = 11.70$, $SD = 7.65$ vs $M = 17.21$, $SD = 7.22$).

Finally, the LOC and BSS subscales were compared between paid and volunteer rescue workers with an independent samples t-test. No significant differences were found (see Table 3).

TABLE 3. The results of LOC and BSS of paid and volunteer rescue workers

Questionnaire	Group	N	M	SD
LOC	Paid	50	10.00	3.25
	Volunteer	50	11.02	3.46
BSS good luck	Paid	50	12.30	8.37
	Volunteer	50	12.64	7.28
BSS bad and changing luck	Paid	50	14.44	7.25
	Volunteer	50	14.78	7.41

4. DISCUSSION

This study aimed to examine the relation of belief in superstition and locus of control among Estonian rescue workers. Roughly one forth of the participants (both paid and volunteer rescue workers) mentioned at least one item they use. It is difficult to estimate whether this proportion is small or large. If we compare it to the available data of religiosity (bearing in mind that religiosity and believing in superstition, including spirituality, are different constructs), then according to the 2011 census in Estonia 29% of population stated that they are religious (Statistikaamet 2017), which is rather a similar proportion in terms of our results.

Locus of control and belief in superstition were positively associated, which is similar to previous findings (see Fluke et al. 2014; Sagone & De Caroli 2014; Todd & Brown 2003; Burke et al. 2006). Also, those participants who mentioned at least one item that brings them luck scored higher in both LOC and BSS (see also Fluke et al. 2014). Thus, the more external the locus of control is, the more one believes in either good, bad or changing luck.

Although previous research has indicated differences between paid workers and voluteers in some domains (Elshaug & Metzer 2001; Lee & Olshfski 2002), there were no statistical differences between the two groups in this study. Also, there were no differences between professional and volunteer rescue workers in LOC and BSS subscales. Thus, we can conclude that persons who either are paid or devote their time and energy by volunteering share similar characteristics in this domain.

As a limitation, it can be pointed out that the sample size was small and not representative to the rescue worker population. Also, as this topic may have been delicate and personal then some of the participants may not have to wished to disclose their items (see also Stone, Bachrach, Jobe, Kurtzman & Cain 2000). The proportion of those rescue workers who mentioned an item was small. Thus, future studies with a larger sample and additional qualitative research methods (for example, interviews) may shed further information on this interesting area of research.

In conclusion it can be said that locus of control and belief in superstition were positively associated. Those rescue workers who mentioned at least one item scored also higher in those two scales. However, there were no differences between professional and volunteer rescue workers in their belief in superstition or in their locus of control.

ACKNOWLEDGEMENTS

The author wishes to thank Gert Teder from the Estonian Rescue Board for collecting and coding the data and Kadi Liik from Tallinn University for her helpful comments.

Contacts:

Kristjan Kask
Tallinn University
School of Natural Sciences and Health
Narva mnt 25, 10120 Tallinn, Estonia
Phone: +372 640 9473
E-mail: kask@tlu.ee

REFERENCES AND SOURCES

Berger, W., Coutinho, E., Figueira, I., Marques-Portella, C., Luz, M., Neylan, T., Marmar, C., and Mendlowicz, M., 2012. Rescuers at risk: a systematic review and meta-regression analysis of the worldwide current prevalence and correlates of PTSD in rescue workers. *Social Psychiatry & Psychiatric Epidemiology*, 47, pp. 1001-1011.

Burger, J. M., and Cooper, H. M., 1979. The desirability of control. *Motivation and Emotion,* 3, pp. 381–393.

Burke, K. L., Czech, D. R., Knight, J. L., Scott, L. A., Joyner, B. A., Benton, S. G., and Roughton, K. H., 2006. An exploratory investigation of superstition, personal control, optimism and pessimism in NCAADivision I Intercollegiate student-athletes. *Athletic Insight: The Online Journal of Sport Psychology*, 8. Retrieved from http://www.athleticinsight.com/Vol8Iss2/Superstition.htm

Campbell, C., 1996. Half belief and paradox of ritual instrumental activism: A theory of modern superstition, *The British Journal of Sociology,* 47, pp. 151-166.

Carlson, B.D., Mowen, J.C., and Fang X., 2009. Trait superstition and consumer behavior: Re-conceptualization, measurment, and initial investigations. *Psychology & Marketing,* 26, pp. 689-713.

Damisch, L., Stoberock, B., and Mussweiler, T., 2010. Keep your fingers crossed!: How superstition improves performance. *Psychological Science*, 21, 1014-1020.

Darke, P. R., and Freedman, J. L., 1997. The belief in good luck scale. *Journal of Research in Personality*, 31, pp. 486–511.

DeVellis, R. F., 2003. *Scale development: Theory and applications* (2nd Ed.). California: SAGE Publications Inc.

Elshaug, C., and Metzer, J., 2001. Personality attributes of voluteers and paid workers engaged in similar occupational tasks. *Journal of Social Psychology*, 141, pp. 752-763.

Fluke, S.M., Webster, R.J., and Saucier, D.A., 2014. Methodological and theoretical improvements in the study of superstitious beliefs and behaviour. *British Journal of Psychology,* 105, pp. 102–126.

Gale, C.R., Batty, G.D., and Deary, I.J., 2008. Locus of control at age 10 years and health outcomes and behavious at age 30 years: The 1970 British Cohort Study. *Psychosomatic Medicine*, 70, pp. 397-403.

Jahoda, G., 1969. *The psychology of superstition*. London: Allen Lane The Penguin.

Keinan, G., 2002. The effects of stress and desire for control on superstition behaviour. *Personality and Social Psychology Bulletin*, 28, pp. 102-108.

Kramer, T., and Block, L., 2008. Conscious and nonconscious components of superstitious belifs in judgment and decision making. *Journal of Consumer Research,* 34, pp. 783-793.

Laherand, M.-L., 2008. *Kvalitatiivne uurimisviis [Qualitative methods].* Tallinn: Infotrükk.

Lee, S.-H., and Olshfski, D., 2002. An examination of variations in the nature of employee commitment: The case of paid and volunteer firefighters. *International Journal of Public Administration*, 7, pp. 29-38.

Lefcourt, H.M., 1982. *Locus of control: Current trend in theory and research*. Hilldsade NH:Erlbaum

Matute, H., Yarritu, I., and Vadillo, M.A., 2011. Illusion of casuality at the heart of pseudoscience. *British Journal of Psychology,* 102, pp. 392-405.

Matute, H., 1994. Learned helplessness and superstitious behavior as opposite effects of uncontrollable reinforcement in humans. *Learning and Motivation,* 25, pp. 216–232.

Ng, W.W.H., Sorensen, K.L., and Eby, L.T., 2006. Locus of control at work: A meta-analysis. *Journal of Organizational Behaviour*, 27, pp. 1057-87.

Päästeamet [Rescue Service]. 2017. Retrieved from www.rescue.ee in 31.07.2017.

Rotter, J., 1966. Generalized expectancies for internal versus external control of reinforcement. *Psychological Monographs*, 80, pp. 1–28.

Rudski, J. M., 2004. The illusion of control, superstitious belief, and optimism. *Current Psychology*, 22, pp. 306–315.

Rudski, J. M., Lischner, M. I., and Albert, L. M., 1999. Superstitious rule generation is affected by probability and type of outcome. *The Psychological Record*, 49, pp. 245–260.

Sachs, J., 2004. Superstition and self-efficacy in Chinese postgraduate students. *Psychological Reports*, 95, pp. 485–486.

Sagone, E., and De Caroli, M. E., 2014. Locus of control and beliefs about superstition and luck in adolescents: What's their relationship? *Social and Behavioral Sciences,* 140, pp. 318-323.

Sild, M., 2004. *Tööstress ja pühendumine tuletõrje- ja päästeorganisatsiooni operatiivtöötajatel [Work stress and commitment in rescue workers].* Tallinn University: Master's thesis in organisation behaviour

Simmons L.C., and Schindler R.M., 2003. Cultural superstitions and the price endings used in Chinese advertising, *Journal of International Marketing*, 11, pp. 101-111.

Sims, M.T., Graves, R.J., and Simpson, G.C., 1984. Mineworkers' scores for the Rotter Internal-External Locus of Control Scale. *Journal of Occupational Psychology*, 57, pp. 327-329.

Statistikaamet [Statistics Estonia]. 2017. Retrieved from www.stat.ee in 01.08.2017.

Stone, A. A., Bachrach, C. A., Jobe, J. B., Kurtzman, H. S., and Cain, V. S., 2000. *The science of self-report: Implications for research and practice*. Mahwah, NJ: Lawrence Erlbaum Associates

Tobacyk J., and Shrader, D., 1991. Superstition and self-efficacy. *Psychological Reports*, 68, 1387-1388.

Todd, M., and Brown, C., 2003. Characteristics associated with superstitious behavior in track and field athletes: Are there NCAA divisional level differences? *Journal of Sport Behavior,* 26, pp. 168–187.

Vyse, S. A., 2000. *Believing in magic: The psychology of superstition*. Oxford, England: Oxford University Press.

THE ROLE OF SOCIALISING AGENTS IN CREATING A SAFER SOCIETY FROM THE PERSPECTIVE OF DOMESTIC VIOLENCE

Silvia Kaugia, Dr. iur.
University of Tartu
Lecturer in Comparative Jurisprudence

Keywords: domestic violence, socialising agents, creating a safer society

ABSTRACT

In 2015, domestic violence accounted for an estimated one-tenth of all crimes, 38% of violent crimes. Since 2011, the proportion of domestic violence crimes has increased steadily in comparison with all other categories of crime, including violent crimes. Domestic violence is at once a social, legal and medical problem that requires cooperation between different organisations and institutions, i.e. interactions, which consider each other's interests and goals. An important factor in prevention and suppression of domestic violence is the attitude towards the victim, both in terms of law enforcement agencies as well as society - the attitude towards victims will have an effect on whether and to what extent victims dare to press charges against perpetrators. The article discusses victim blaming through the eyes of the victims themselves as well as the population (using sociological surveys) and determines, if and to what extent victim blaming attitudes can affect the cover-up in cases of domestic violence and retraction of testimonies in criminal proceedings. Victim blaming may to a larger or a lesser extent also hinder the cooperation between victims and law enforcement agencies and affect both criminal proceedings as well as trials.

The attitudes to domestic violence and to those involved are constantly changing over time. Acceptance of changes in society is a time consuming process, where various institutions-socialising agents have their roles to play. The article identifies the role of family, school and the media in fighting domestic violence and contributing to positive changes.

1. DESCRIPTION OF THE PROBLEM

Domestic violence is widespread and on the rise in Estonia. In 2015, 2997 domestic violence cases were registered, an increase of one tenth compared to 2014 and 55% more than in 2011. In 2015, domestic violence was estimated to constitute one-tenth of all crime, and 38% of violent crime.[1] An estimated 3017 cases of domestic violence were registered in 2016, which is 20 more than in 2015. As for the last six years, the number of domestic violence crimes peaked in 2016, but its growth has slowed down compared to 2012, 2013, and 2015. In 2016, domestic violence constituted for a tenth (10.4%) of all crime and 39% of violent crime cases. Since 2011, the proportion of domestic violence crimes has steadily increased compared to both all crime and violent crime specifically.[2] Understandably, the statistics reported reflect the number of registered cases of domestic violence. (Table 1).

TABLE 1. Number of registered cases of domestic violence per year

Year	Number of cases
2012	2231
2013	2752
2014	2721
2015	2997
2016	3017

Given that a large number of domestic violence cases are latent, one can conclude that there is no sign of a marked decline in this type of violence in society, even if the cases of domestic violence were to be linked to different types of cases of abuse (and to statistics). First of all, it is important to emphasise the nature of domestic violence as a specific type of violence - it takes place in close (intimate) relationtionships and is systematic by nature. (See the concept of domestic violence via the link to

[1] Justiitsministeerium, "Kuritegevus Eestis 2015." (The Ministry of Justice, Estonia 2015 Crime in Estonia 2015) (2016), pg 34, (in Estonian) < http://www.kriminaalpoliitika.ee/sites/krimipoliitika/files/elfinder/dokumendid/kuritegevus_eestis_2015.pdf > (09.08.2017).

[2] Justiitsministeerium, "Kuritegevus Eestis 2016". (Crime in Estonia 2016) (2017), pg 41, (in Estonian) <http://www.kriminaalpoliitika.ee/sites/krimipoliitika/files/elfinder/dokumendid/kuritegevus_eestis_est_web_0.pdf> (09.08.2017).

the Instanbul Convention). Thus, the equation of the cases of domestic violence with any other violent crime is not justified. As far as criminal statistics are concerned, it relates to penal policies: "compared to 2015, the number of recorded gross violations of public order (+715, +166%) saw a sharp increase in 2016; meanwhile the number of recorded crimes of physical abuse decreased (–834; –15%) - as a result of major changes in procedural practices - starting from spring 2015, violent crimes committed in public are registered as gross violations of public order instead of physical abuse. Therefore, the number of criminal offenses registered under § 263 of the Penal Code has increased and the number of criminal offenses registered under § 121 of the Penal Code has decreased accordingly". [3]

The main elements of domestic violence crimes are covered by Part 2 of the Penal Code (violent offences), which currently include two articles: § 120 – threat and § 121 – physical abuse. Amendments to the Penal Code, in force as of January 1, 2015, (§ 121 lg 2 p 2) stipulate stricter punishment for physical abuse carried out in intimate partnerships or against dependants. This is also the sole article of the Penal Code referring to domestic violence. It is important that domestic violence as a term has been included in the existing laws, which reflects the need to differentiate between domestic violence as a specific form of violence and other types of violence.

Besides Article 121 of the Penal Code, all articles of the Penal Code including the element of violence are used to charge perpetrators of violence. Threat to kill, cause health damage or cause significant damage to or destroy property, if there is reason to fear the realisation of such a threat, causing damage to the health of another person, or beating, battery or other physical abuse which causes pain, continuous physical abuse or physical abuse which causes great pain, are all punishable as criminal offences.

Indeed, physical maltreatment incidents predominated in Estonia in 2015 among domestic violence cases: 85% out of all domestic violence crimes and 45% out of all physical maltreatment cases (in 2014 respectively 79%

[3] Justiitsministeerium, "Kuritegevus Eestis 2016" (The Ministry of Justice, Crime in Estonia 2016). (2017), lk 33, <http://www.kriminaalpoliitika.ee/sites/krimipoliitika/files/elfinder/dokumendid/kuritegevus_eestis_est_web_0.pdf> (23.09.2017).

and 40%).Compared with 2014 the share of physical maltreatment in intimate partner relationships has increased in domestic violence and all cases of physical maltreatment, which primarily can be explained with the abolition of the crime of torture. Compared with 2014, the share of domestic violence cases in threatening and sexual crimes has slightly declined. The share of manslaughter and murder in intimate partner relationships out of all crimes qualified according to Articles 113-114 of the Penal Code was 20%. According to the police the share of manslaughter and murder related to domestic violence remained the same compared to 2014. According to preliminary data, 10 cases of manslaughter or murder related to domestic violence were registered in 2015, resulting in the death of five individuals. Approximately 2/3 of domestic violence cases are related to the violence of current or former spouses/partners, but there are also cases of parental violence against children or stepchildren (altogether 14%) and children's violence against parents (9%).[4]

In 2016, physical abuse accounted for the highest proportion of domestic violence crimes (85%). Domestic violence crimes consituted more than half of the all crimes of physical abuse. Compared to 2015, the proportion of physical abuse related to domestic violence has grown by almost 8% out of all crimes of physical abuse - this is a result of major changes in procedural practice. On January 1, 2015, amendments to the Penal Code § 121 (2) 2) entered into force, stipulating a more severe term of punishment for physical abuse committed in close or dependency relationships. In 2016, about 520 individuals were convicted under this provision. The number of other types of crimes committed under the domestic violence category is significantly lower. Threats, for example accounted for one-tenth of domestic violence crimes in 2016, sexual crimes 3% and offences against life and health (killing, murder, serious physical harm) slightly more than 1%. According to preliminary data from the police, 9 domestic violence connected killings, murders and related attempts were registered in 2016, which is one less than in 2015.[5] In the estimation of the author, the percentage of domestic violence and other violent

[4] Justiitsministeerium, "Kuritegevus Eestis 2015." (The Ministry of Justice, Estonia 2015 Crime in Estonia 2015) (2016), p 35, (in Estonian) < http://www.kriminaalpoliitika.ee/sites/krimipoliitika/files/elfinder/dokumendid/kuritegevus_eestis_2015.pdf > (09.08.2017).

[5] Justiitsministeerium, "Kuritegevus Eestis 2016"(The Ministry of Justice, Crime in Estonia 2016). (2017), lk 42. <http://www.kriminaalpoliitika.ee/sites/krimipoliitika/files/elfinder/dokumendid/kuritegevus_eestis_est_web_0.pdf> (23.09.2017).

crime statistics is proportional - the number of killings and murders has decreased in both categories of crime statistics. The author also finds that killings and murders are not the key indicators in domestic violence statistics, all the more so because domestic violence is not always physical in nature.

According to the World Health Organization (WHO), domestic violence involves all forms of violent aggression, psychological harassment, forced sexual intercourse and other acts of sexual coercion, as well as social control, which results in one person being isolated from the rest of the world, including one's own family. [6]

In addition to physical violence, forms of psychological, sexual and economic violence are also distinguished as types of domestic violence. Obviously, there is a reasonable assumption that the main latent part of domestic violence falls under these last three types, as the current legal system lacks the relevant provisions for these types of domestic violence.

As domestic violence[7] is simultaneously a social, legal and medical problem, solutions require the cooperation of different organisations and institutions. The issue falls mainly under the competence of law enforcement agencies, social workers, child protection workers, medical personnel and the staff of women's shelters. Less attention has been paid to what the family, school and media, as important socialisation agents, and what society as a whole can do to prevent and combat domestic violence.

It is not possible to overestimate the effect of socialising agents in preventing and combating domestic violence - as their main tasks are: 1) *shaping a person*, starting with the fact that the child is made aware of what is good and what is bad, what should and should not be done; 2) *affirming positive social attitudes* - specific (legal) education will affect

[6] Intimate partner violence. World Health Organization. <http://www.who.int/violence_injury_prevention/violence/world_report/factsheets/en/ipvfacts.pdf> (23.09.2017).

[7] *Domestic violence* (also referred to as intimate partner violence) *shall mean all acts of physical, sexual, psychological or economic violence that occur within the family or domestic unit or between former or current spouses or partners, whether or not the perpetrator shares or has shared the same residence with the victim*. See Council of Europe Convention on preventing and combating violence against women and domestic violence Art. 3. Istanbul, 11V. 2011. <https://www.coe.int/t/DGHL/STANDARDSETTING/EQUALITY/03themes/violence-against-women/Conv_VAW_en.pdf> (09.08.2017).

the consciousness and behavior of a person when he or she has already achieved a certain social maturity and is able to understand the content of different behavioral norms; 3) *establishing the basis for the rational choice behavior* - a person selects information from the socialisation agents about the correct behavior and shapes his or her behavior on the basis of such information; 4) *introducing the principles of social behavior* - all forms of social relations require contacts between members of society, whereupon various types of relationships between people are formed and developed. Regardless of the nature of a relationship, individuals affect each other through every interaction, striving to get the other person "to tune into their frequency" so-to say, and adapt that person (and, if possible adapt themselves) to "the game rules" of that relationship; 5) *improving self-control in the system of social control* - mutual coordination of the behavior of individuals and social groups; 6) *developing advanced behavioral-regulatory legal consciousness* – directing people (especially young people) to the internalisation of social values, that is to say, their acceptance of the level of consciousness; 7) *guiding individuals towards lawful behavior* - by trying to solve this task through the dissemination of legal knowledge and intensification of legal propaganda, we should not forget that the mere knowledge of the law, without the support of deeper behavioral regulators, cannot ensure the legitimate conduct of an individual. The psychological aspect of an individual is the starting point for identifying the causes of a norm-abiding behavior[8].[9]

Therefore, quite a lot of subjective regulators of human behavior (including legally meaningful regulators) are internalised through direct imitation and identification of legal knowledge. This means that by the time that a person comes of age when his or her legal consciousness can be shaped through the provision of legal knowledge, the basic structure of legal consciousness has already developed. However, the quality of this structure depends on the behavioral patterns that the person has imitated previously or with whom the person has identified with in his

[8] Of course, the state will also use the means at its disposal (sanctions and their application, the development and implementation of general and special prevention methods, etc.) to ensure that subjects of law comply with the law, but the behavior of a person is still mainly based on mental models of behavior that he or she consciously or less consciously associates to real behavioral standards.

[9] See more Kaugia, S. "Õigusteadvuse olemus ja arengudeterminandid" (2011) (Essence of Legal Consciousness and Determinants of Development), pg 73-85.

or her behavior. The higher the level of human legal consciousness, the more justified is the hope that in any living situation, he or she opts for a norm-abiding behavioral variant. Here lies the key to the success for well-coordinated socialisation agents - shaping a person's attitudes, behaviors, and offering knowledge of norm-abiding behaviors that, in their totality, create the basis for developing behavioral tendencies for a safer society.

2. THE MOST IMPORTANT FORMAL AND INFORMAL SOCIALISATION AGENTS AND HOW THEY CAN HELP TO CONTROL FAMILY VIOLENCE

Socialisation is a process between a social environment and an individual, in which the individual acquires a system of knowledge, norms and values that enables him or her to be a full member of society. The socialisation process is carried out through socialising agents. It is a lifelong process, during which the socialisation agents will change, and so will the significance of their impact and importance. The socialisation process of a person has several agents acting at the same time, some of which have a dominant, and others a secondary role. While different socialisation agents have a different effect on the socialised person, they relate directly to the acceptance and internalisation of social norms (i.e., acceptance at the level of consciousness). The impact of various socialisation agents on human development depends on these agents' level of authority for that particular person. The influence and authority of socialisation agents changes over time. Socialisation agents represent a connecting link between the subject and society and their role is not to be underestimated. In the context of this writing, the unavoidable social integration aspects are the formation of social justice attitudes, the guidance of the rational choice behavior and the awareness of the need for self-control. The extent to which the legal consciousness of a person (legal awareness) and their actual behavior coincides, depends on the role models that the person has identified with or imitated in their

behavior, that is to say, with the socialisation agents which are important for that person.[10]

While socialisation agents can be classified in various ways, this paper focuses on formal and informal agents.

2.1. Formal socialisation agents for the prevention and combating of family violence

The most important formal socialisation agent is the state, as well as national organisations and institutions whose role in socialising is limited to their specified competence.

The state has many alternatives for controlling domestic violence; these relate to the expectations and hopes of society. The state's capacity to deal with domestic violence cases is the key in ensuring the victims security and preventing domestic violence. There are several parameters for assessing this, the most important of which were added in an expert review[11] survey prepared by the Estonian Open Society Institute and UT Institute of Public Law in 2014. [12]

The results of the survey (Table 2) indicate that opinions on the capacity of the state vary. People are most satisfied with the treatment of victims by the legal authorities, as well as ensuring the safety of victims' children. However, respondents also stated that several key issues remain unresolved.

---

[10] Kaugia, S. "Õigusteadvuse olemus ja arengudeterminandid" (2011) (Essence of Legal Consciousness and Determinants of Development), pg (138-139.

[11] In November and December of 2014, a nationwide expert survey of legal practioners was organised by the Norwegian Financial Mechanism and the Estonian Ministry of Social Affairs, entitled "Building an integrated system for combating intimate partner violence in Estonia" which received responses from 203 specialists: 122 practicing lawyers (prosecutors, lawyers, judges and other legal professionals) and 81 police investigators. The research methodology was developed by the Estonian Open Society Institute (Ivi Proos and Iris Pettai) in cooperation with the Institute of Public Law of the University of Tartu (Silvia Kaugia, Raul Narits, Jüri Saar), with consultations by Kati Arumäe of the Police and Border Guard Board.

[12] See Pettai, I., Narits, R., Kaugia, S, "Of the Current State and Outlook of the Legal Regulation on Domestic Violence Based on the Results of an Expert Poll Carried Out Among the Estonian Legal Practitioners" – IX, *Juridica* (2015), pg 645-658.

TABLE 2. What do you think of the capacity of the Republic of Estonia in dealing with cases of domestic violence? (%)

	Prosecutors		Judges		Police investigators	
	Good+ satis-factory	Poor	Good+ satis-factory	Poor	Good+ satis-factory	Poor
I. High capacity						
Ensure safe and fair treatment of victims by law enforcement agencies	91	7	64	28	82	10
II. Medium capacity						
Ensure the safety of victims' children	60	33	48	40	56	41
III. Low capacity						
Prevent family violence and serious incidents	33	60	12	72	38	58
Supervise violent families	29	62	16	72	28	68
III. Very low capacity						
Have an overview of perpetrators and to manage them	19	71	16	68	27	70
Provide victims with subsistence allowance and material conditions to cope independently	10	74	16	88	10	81

Source: Estonian Open Society Institute, 2014

The majority of respondents (58-72%) find that the state is unable to prevent domestic violence and avoid serious incidents, and assert that there is no control over perpetrators of violence (60-68%) and violent families (60-68%). According to experts, the total failure of the state is indicated by its inability to provide survivors with support payments and ensure other material conditions that would allow them to cope independently: 88% of judges, 81% of police investigators and 74% of prosecutors deem the state support insufficient. The study shows that judges are somewhat more critical of the abilities of the state.[13]

[13] It would appear that the requirements for the "Development Plan for Reducing Violence for 2010-2014" have not been fully realised in Estonia. This is evidenced by the "Violence Prevention Strategy 2015-2020", in which a number of bottlenecks are highlighted alongside the positive outcomes of the development plan: prevention of violence is not consistent and systematic; professionals can not recognise the signs of violence; services for victims do not cover all the needs of victims; the safety of child victims is not always guaranteed; law enforcement cannot always prevent secondary victimisation; statistics on victims and perpetrators of violence are flawed and not readily available. <https://valitsus.ee/sites/default/files/content-editors/arengukavad/vagivalla_ennetamise_strateegia_2015-2020_kodulehele.pdf> (09.08.2017).

The experts' answers suggest that the capacity of the state is lower in those aspects related to the prevention of domestic violence, and higher in the areas dealing with its consequences. It would probably be wise to concentrate more on the cooperation between local governments and the state, and increase the role of the local level. This is also indicated in Item 7 of the appendix to the Riigikogu resolution of June 9th 2010, which notes that *crime prevention must primarily occur at the local level. The task of the local government is to reduce the factors fostering crime by involving local residents and the private and non-profit sector*[14].

There is no separate family violence law in Estonia, and this may be one of the reasons why we primarily deal with the consequences of violence, and less with prevention of violence. Such law would give a strong signal to society that the state condemns family violence and acts of domestic violence will have more sanctions. The latter requirement stems directly from the Istanbul Convention[15], which Estonia has signed and which is to be ratified in the near future.

We have made a number of suggestions in the legal literature for the development of this law.[16] The more developed the society and the more there are different institutions and cooperations between them, the more effective the prevention of domestic violence as well as combating the manifestations of domestic violence will be.

The task of formal socialisation agents is to serve the interests of society by providing solutions for organising damaged social relationships.

---

[14] Justiitsministeerium, "Kriminaalpoliitika arengusuunad aastani 2018." (The Ministry of Justice, Estonian Guidelines for *Development* of Criminal Policy until 2018.) (in Estonian) <www.just.ee/sites/www.just.ee/files/elfinder/article_files/kriminaalpoliitika_arengusuunad_aastani_2018.pdf > (29.07.2015).

[15] Euroopa Nõukogu naistevastase vägivalla ja perevägivalla ennetamise ja tõkestamise konventsioon. (Istanbuli konventsioon). Istanbul, 11V.2011. (Council of Europe Convention on preventing and combating violence against women and domestic violence. (I.e. the Istanbul Convention)) (in Estonian) <https://rm.coe.int/1680462531> (09.08.2017).

[16] Pettai, I., Kaugia, S., Narits, R. "Perevägivald nõuab jõulisemat juriidilist sekkumist" – *Riigikogu Toimetised*, 31, 2015, lk 155 – 167; Pettai, I., Narits, R., Kaugia, S. "Perevägivalla juriidilise regulatsiooni hetkeseis ja perspektiiv Eesti õiguspraktikute küsitluse põhjal" – *Juridica*, IX, 2015, lk 645-658; Narits, R., Kaugia, S., Pettai, I. "The Significance of Recognising Domestic Violance, in Light of Estonian Legal Experts´ Opinion and the Prospects for Systematising the Relevant Legislation" – *Juridica International* 24, 2016, pp 128-138.

However, it is not right to underestimate the role of society (i.e. various non-formal socialisation agents) in guaranteeing social security.

2.2. Non-formal socialisation agents for preventing and combating domestic violence

One of the most important means available to society for ensuring social security is to improve the level of socialisation and thereby ensure the social integration of different social groups. Non-formal socialisation agents are primary and their role is invaluable in the prevention of domestic violence - attitudes, views and perceptions that develop on the social level, become important guides of human behavior. When society still holds on to the stereotype that the victim of domestic violence has brought it upon themselves, law enforcement agencies continue to face problems in dealing with this type of violence. Uncertainty and fear of accusations are one of the reasons why a woman suffering violence rarely dare to turn to law enforcement agencies. A study by the European Union Agency for Fundamental Rights on violence against women revealed that only 14% of women turn to the police even after the most serious incidents (10% in Estonia). Only one in three women seeks medical attention after violent incident, 4-6% seek help from women's shelters or from victim support.[17]

According to the EMOR survey conducted in 2014, more than half (54%) of the respondents consider victims of domestic violence partly at fault and almost half (47%) consider that women are to blame for their own rape based on the clothes they wear.[18]

[17] A total of 4,200 women were surveyed throughout the EU. See Violence against women: an EU-wide survey. Main results report .FRA (2014). <http://fra.europa.eu/sites/default/files/fra-2014-vaw-survey-main-results-apr14_en.pdf> (10.08.2017).

[18] Sotsiaalministeerium. "Eesti elanikkonna teadlikkuse uuring soopõhise vägivalla ja inimkaubanduse valdkonnas. Uuringu aruanne". TNS EMOR (2014). (The Ministry of Social Affairs. Attitudes of Estonian inhabitants in relation to gender-based violence and human trafficking. Survey report.) (in Estonian) <https://www.sm.ee/sites/default/files/content-editors/eesmargid_ja_tegevused/Norra_toetused/Koduse_ja_soopohise_vagivalla_vahendamise_programm/elanike_hoiakud_soopohise_vagivalla_ja_inimkaubanduse_valdkonnas2014_aruanne_tns_emor_loplik.pdf> (10.08.2017).

In the previously referred expert survey of 2014, 67-71% of respondents supported the perception that reckless women who hitchhike with strangers, get drunk, and go along with strange men, bring violence upon themselves with their careless and foolish behavior. Another widespread belief is that women nag men until men finally break and hit their partners. This position was supported by 60-76% of respondents. The attitude that women fall victim to sexual violence primarily because of their provocative behavior and clothes, received much less support from experts - only 24% of prosecutors, 40% of judges and 42% of police investigators were in agreement. (Table 3).

TABLE 3. Why do women fall victim to physical or sexual violence? (Answers to the scale item "especially + as") (%)

	Prosecutors	Judges	Police investigators
I. It is the fault of women who...			
...are careless – hitchhike in random cars, get drunk, go along with unfamiliar men	69	72	71
... provoke men to violence by their constant nagging	76	60	75
... provoke men with their provocative behavior, clothes	24	40	42
II. It is the fault of men who...			
... do not control their aggression, have rage issues and become quickly violent when angered	98	96	97
... try to control everything, to enforce their will and to put women in their place	95	88	97
III. Violence is caused by			
alcohol, drugs	95	84	96
unemployment	62	48	79
poverty	60	56	70

Source: Estonian Open Society Institute, 2014

Prevention of domestic violence begins primarily by encouraging victims to seek assistance from an appropriate organisation. Victims need to be assured that their problem will be addressed. Cooperation between different organisations must be improved in order to avoid situations in which the victim is forced to talk about the problem to different institutions and to re-live the experience repeatedly. These changes would

contribute to ensuring the victim's security, which is something that remains within the competence of both the state and social organisations.

Socialisation by external forces is inextricably linked to the concept of self-socialisation. In the latter case, the determining factor in the development of personality is the environment of a person - this leads to the comprehensive development (legal consciousness, behavioral tendencies, norm-abiding, etc.) of a person and whether a person supports or obstructs the actions of socialisation agents. Both the environment and the socialisation agents may either be of a norm-abiding or anti-normative nature.

In the socialisation process, particular emphasis should be placed on the development of children and young people – the formation of a person begins at birth, and their upbringing creates the basis for all further social behavior. The feedback that a person receives (particularly in childhood) on his or her behavior has a direct impact on their level of legal consciousness and behavioral patterns. This is why free parenting of children and consequent deprivation of evaluative and emotional relationships with their parents and other close relatives cannot be accepted. A violent family or a family where violent behavior is accepted irrespective of location, is another serious risk for the development of a norm-abiding individual. "The family model that implements violence is acquired in childhood and can be repeated from generation to generation".[19]

Domestic tensions caused by various factors may be manifested in many different forms of family violence, which, as a rule, also involve the child. In addition to seeing violence, children are also at immediate risk of falling victim to physical, mental or sexual violence: they may be immediate victims of a violent family (violence aimed at them), see or hear violence among other members of the family, may accidentally fall victim to violence aimed at other persons, may become involved in violence against another person (for example, manipulation of children by another parent). [20]

[19] Gustafsson, M. et al. "Intimate Partner Violence and Children's Memory" – Journal of Family Psychology, (27) 6, 2013, p 937.

[20] Laps perevägivalla ohvrina. <http://abiksohvrile.just.ee/et/lapsele/laps-perev%C3%A4givalla-ohvrina> (25.09.2017).

From the viewpoint of a child, domestic violence creates lasting damage to the psyche of the child and guides the child to other forms of violence (such as school violence and development of general cruelty). The view that violence generates violence holds true here: a child who sees parental hostilities or physical abuse at home, will, on one hand, grow up believing that such behavior is normal (even traditional in its mundaneness) and may practice it easily on their peers or animals or birds, and on the other hand, it may provoke fear and frustration in a child, which creates a real risk that the child him- or herself may become a target of any kind of violence.

The family is simultaneously a socialisation agent and a socialisation environment, which means that it is crucial in terms of accepting norms at the level of consciousness. The family (home) should be the place where a person can feel secure, where he or she feels safe. If this is not the case, then the foundation of personality development is missing the most important brick that is needed to build a strong load-bearing construction.

This is why more attention should be placed on combatting family violence, and the main intent must of course come from the families themselves. This has been a topical issue for years – the Ministry of Justice outlined the following important actions in their 2012 development plan: "To reduce domestic violence, actions are planned mainly in two areas: raising legal awareness and informing the public about family violence, and harmonising the procedure for domestic violence cases. The action plan sets an objective for 2012 to amend social education books and to train social education teachers in order to cover topics of domestic violence, non-family (i.e. gender-based) violence and opportunities for helping victims of violence. Regular surveys on procedural practice are carried out both at the Ministry of Justice's Department of Analysis and in the Police and Border Guard Board. This will help to identify potential regional differences and bottlenecks in procedural practice. Analyses will be supplemented by meetings between police officers and prosecutors that allow the practice to be improved and harmonised. If necessary, these roundtables may set out common working principles or additional guidance for standardising practice. An analysis of the domestic murders will also be carried out (the criminal statistics are used to analyse

how many killings and murders have been related to previous domestic violence cases).[21] All this remains topical even today.

The author finds that it is very important to address the problem at the national level, however, that does not provide real and quick solutions for improving the situation. A more realistic option would be to raise the awareness of the population to the seriousness of family violence. This increase in public awareness could hypothetically also make people want to have more control over their behavior and, in the case of family conflicts, find quick answers and solutions that would spare children, in particular. Efforts should be made to ensure that the next generations will be more capable of solving problems as civilised people, not with fists and mental abuse. Conscious development of related (legal) awareness should help here. It must be emphasized that in this context, awareness raising is meant as raising the level of legal consciousnes, which includes views, attitudes, knowledge and the behavioral trends that are formed upon them. These elements form the so-called classical structure of legal consciousness.

Today the family can no longer fulfill all the traditional tasks in raising young people. This is why other socialising agents have also emerged in order to pass on the rules of conduct and cultural values in society. One of these relevant institutions is school, which is responsible for helping young people grow up in accordance with the behavioral expectations of society. The school is a place where socialisation is both a goal and an educational activity at the same time. The school is an organisation that plays an important role in the socialisation of students. It is a bridge between two important stages: socialisation in the home environment and socialisation in a social environment[22].

The functions of the school change with societal changes and developments, and another thing that changes, is its prestige in the eyes of young people. The latter will have an impact on the extent of the influence that

[21] Justiitsministeerium, "Vägivalla vastu võitlemise arengukava aastateks 2010-2014. 2011.a täitmise aruanne" (2012), < www.just.ee/orb.aw/class=file/action=preview/id=56652/V%E4givalla+V%Ehend> (24.10.2012). (The Ministry of Justice. *Development Plan* for Fighting against Violence 2010-2014. 2011 Report on the Implementation) (in Estonian)

[22] Risnoveanu, A. "The Students' Socialization – A Real and Actual Challenge for the School Organization" – *Journal of Educational Sciences & Psychology*, LXII, No 1B/2010, p 73.

school has as a socialising agent at various stages of societal development. It is important to emphasise the close link between the school and the home as socialising agents.

During the last decade, major changes have taken place in the educational system of Estonia, in the content of learning, in the system of educational institutions and in the organisation of education as a whole. The national framework curricula for school education has given schools the right and obligation to develop a school curriculum that allows for school specialties, interests of students and regional specificities to be taken into account[23]. This has allowed schools to add several optional courses to the curricula. For example, the curriculum of Tartu Kristjan Jaak Peterson Gymnasium[24], which allows students to choose a legal education module. In the context of this article, the most important aims of this module are: to deepen the understading of justice and legal consciousness in young people, tolerance and honesty in their relations with other people; to develop skills essential in the field of effective legal behavior, such as critical thinking, analysis, communication, observation and problem solving skills; to achieve that the student understands, values and protects human rights and fundamental freedoms, respects the principles of democracy and democratic values, and observes generally accepted rules of conduct.[25]

Paragraph 8 (5) of the National curriculum for upper secondary schools[26] provides a list of compulsory and optional courses in the field of social sciences. Social science courses discuss how people and societies have functioned both in the past and today.

The tasks of the modern school include, using social sciences, to teach students causal and other similar relationships in the development of society and how to make informed choices in relation to their own and

[23] Märja, T. "Euroopa Liidu hariduspoliitika mõjutused Eestis" – *Eesti ja Soome haridus ning muutused EL-i hariduspoliitikas 1990-2000. Artiklite kogumik*. L. Jõgi, T. Jääger, R. Leppänen, R. Rinne (Koost). (2008), lk 308, 310.

[24] Tartu Kristjan Jaak Petersoni Gümnaasiumi õppekava (The Curriculum of Tartu Kristja Jaak Peterson Gymnasium) (2016). < https://kjpg.tartu.ee/img/image/Dokumendid/KJPG_oppekava_20161.pdf> (25.09.2017).

[25] *Ibid,* lk 319.

[26] Gümnaasiumi riiklik õppekava. (National curriculum for upper secondary schools.) 06.06.2011. – RT I, 14.01.2011, 2; RT I, 29.08.2014, 21.

the surrounding social environment, based on the values and morals of society and how to act as moral and responsible persons and members of society. Mandatory courses are history, social education, personal education and geography. Upper secondary school students can choose the option "Human and Law". The aim of the course is to develop students' understanding of the dynamics of law and which skills to use in legal situations[27].

Nowadays the lives of young people are increasingly spent outside the narrow family circle. In addition to the family experience, young people are also influenced by school, and particularly by relationships with other students and teachers: friendly and well-meaning relationships will undoubtedly have a positive effect – showing that every young person is valued, wanted and popular. On the other hand, humiliating and ridiculing can create an inferiority complex in a young person, lower their self-esteem, and give birth to aggression and a desire to "take revenge on the whole world." The latter can also have a significant effect in turning young people to crime. Home and school should cooperate more in order to reduce violence. Burying our heads in the sand does not solve the problem.

Kindergarten has an increasingly important role to play as a socialising agent in the prevention of domestic violence. It is the opinion of the author that along with family and school, kindergarten can safely be placed in the list of major socialising agents for children. The kindergarten, the same as the family, also shapes and cultivates a person in their early childhood; at the same time, the kindergarten has a national curriculum[28] with the same socialisation methods as the school.

A young persons ability to cope in society and their behavioral patterns (including violent behavior), largely depends on their self-esteem, which either inspires or inhibits their actions and guides their behavior. Self-esteem is the product of socialisation, which is formed based on influences from the family, school and social environment.

---

[27] Seletuskiri gümnaasiumi riikliku õppekava määruse eelnõu juurde. 05.01.2010, pg 37, 39 (Explanatory note to the draft regulation of upper secondary school curriculum.) (in Estonian) <https://www.hm.ee/sites/default/files/2010._aasta_pohikooli_oppekava_seletuskiri.pdf> (10.08.2017).

[28] Koolieelse lasteasutuse riiklik õppekava. – RT I 2008, 23, 152.

Another extremely important influence in the development of a person is the media (television, radio and print media (as the main types of mass communication), as well as the internet). The information that we receive from these channels should be true and reflect the position of the society with the regard to the events that have taken place. In order for mass communication as an influential institution to successfully fulfill the role of a (legal) socialising agent, particular attention should be paid to the quality of this institution. Unfortunately, not everything that reaches the recipients of the mass media, i.e. the members of society, is educational, edifying, aesthetical or ethical. What's more: violence, which is constantly promoted (especially through films shown on television), attracts imitation, deaths shown in TV shows or in cinemas do not cause horror or fear, and rather sound like a fun thing try on others. This is especially true of young people who hit, beat or even torture (cases of school violence that have become public) their peers and feel nothing for their victims, nor can imagine being in the place of their victims, and instead enjoy their power over them. Everything happens so easily - "just like in the movies". This statement refers to the great role of the media and its capabilities in preventing family violence. This even despite the fact the media of today has become primarily a business for profit.

The purpose of the mass media is to shape people's values. Although their impact is stronger, more decisive and more visible to young people, the mass media undoubtedly helps adults to acquire role models, whom they follow in the ever-changing social environment. It is not an exaggeration to say that the mass media is a strong power (the so-called "fourth power" in addition to the legislative, executive and judicial branch), which plays an important role in shaping people's legal knowledge and guiding their behavior. As a socialisation agent, the media could be more effective by limiting the transmission of violence-promoting material. There is already enough violence in society, perhaps the media, using the means at their disposal, should try to provide more positive emotions.

All of these socialisation agents are crucial for helping to make positive changes in the management of domestic violence. The key point here is to change the attitudes towards victims: if the victims of domestic violence continue to also be perceived as the perpetrators of domestic violence, then it will not be possible to reduce the violence in a meaningful way. This is because it will not be possible to determine who needs protection

in a domestic dispute. Changing the societal attitudes towards the victims and the perpetrators of domestic violence may take a long time because of existing stereotypes, and these changes may also be guided by the state via legislative drafting.

THE FINAL WORD

Family violence is not a problem that should only be addressed if the statistics for domestic violence crimes go up. This is a key issue, and its resolution requires cooperation between different organisations. Cooperation is also needed between different socialisation agents. Unfortunately, there is still a lot to be done here: the institutions often try to delegate their tasks to others. A good example here is the link between the home and the school - both of them can reveal the shortcomings of one another while being incapable of critical self-analysis. Cooperation between them is extremely important, unfortunately it can be hindered by both formal and non-formal factors.

The shared aim of the socialisation agents (should certainly be) the raising and developing of norm-abiding, conscience, self-control. It is important to achieve harmony between individuality and social behavior: nonviolent behavior must be a conscious act, often requiring self-transcendence. Whether and to what extent we are able to control our behavior depends on the quality of the actions of the socialisation agencies and indicates their success.

The specific task of socialising agents is to control the role of the birth factor in the social behavior process and help to adapt individuals to the social environment. An important objective to strive for is to ensure that society would have as few individuals as possible who are not able to control their internal reactions during social interactions, that is, whose self-control does not function at the required level (i.e. the level that would be required for the stable functioning of the society).

A prerequisite for effective prevention may be the awareness and elimination of potential danger signs that can evolve into domestic violence. There is no ideal formula for preventing or stopping domestic violence,

the effectiveness depends on the various factors coming together. The more developed the society and the more diverse the organisations and the better the cooperation between them is, the more effective the fight against domestic violence will be, which in turn will contribute to the security of society.

Contacts:

Silvia Kaugia
Näituse 20-322, 50409 Tartu, Estonia
Phone: +372 5384 9325
E-mail: silvia.kaugia@ut.ee

REFERENCES AND SOURCES

A total of 4,200 women were surveyed throughout the EU. See Violence against women: an EU-wide survey. Main results report .FRA (2014). <http://fra.europa.eu/sites/default/files/fra-2014-vaw-survey-main-results-apr14_en.pdf> (10.08.2017).

Council of Europe Convention on preventing and combating violence against women and domestic violence Art. 3. Istanbul, 11V. 2011. <https://www.coe.int/t/DGHL/STANDARDSETTING/EQUALITY/03themes/violence-against-women/Conv_VAW_en.pdf> (09.08.2017).

Euroopa Nõukogu naistevastase vägivalla ja perevägivalla ennetamise ja tõkestamise konventsioon. (Istanbuli konventsioon). Istanbul, 11V.2011. (Council of Europe Convention on preventing and combating violence against women and domestic violence. (I.e. the Istanbul Convention)) (in Estonian) <https://rm.coe.int/1680462531> (09.08.2017).

Gustafsson, M. et al. "Intimate Partner Violence and Children's Memory" – *Journal of Family Psychology,* (27) 6, 2013.

Gümnaasiumi riiklik õppekava. (National curriculum for upper secondary schools.) 06.06.2011. – RT I, 14.01.2011, 2; RT I, 29.08.2014, 21.

Intimate partner violence. World Health Organization. <http://www.who.int/violence_injury_prevention/violence/world_report/factsheets/en/ipvfacts.pdf> (23.09.2017).

Justiitsministeerium, "Kriminaalpoliitika arengusuunad aastani 2018." (The Ministry of Justice, Estonian Guidelines for *Development* of Criminal Policy until 2018.) (in Estonian) <www.just.ee/sites/www.just.ee/files/elfinder/article_files/kriminaalpoliitika_arengusuunad_aastani_2018.pdf > (29.07.2015).

Justiitsministeerium, "Kuritegevus Eestis 2015." (The Ministry of Justice, Estonia 2015 Crime in Estonia 2015) (2016), (in Estonian)

< http://www.kriminaalpoliitika.ee/sites/krimipoliitika/files/elfinder/dokumendid/kuritegevus_eestis_2015.pdf > (09.08.2017).

Justiitsministeerium, "Kuritegevus Eestis 2016" (The Ministry of Justice, Crime in Estonia 2016). (2017),

<http://www.kriminaalpoliitika.ee/sites/krimipoliitika/files/elfinder/dokumendid/kuritegevus_eestis_est_web_0.pdf> (23.09.2017).

Justiitsministeerium, "Vägivalla vastu võitlemise arengukava aastateks 2010-2014. 2011. a täitmise aruanne" (2012),< www.just.ee/orb.aw/class=file/action=preview/id=56652/V%E4givalla+V%Ehend> (24.10.2012). (The Ministry of Justice. *Development Plan* for Fighting against Violence 2010-2014. 2011 Report on the Implementation) (in Estonian)

Justiitsministeerium, "Vägivalla vastu võitlemise arengukava aastateks 2015-

2020". <https://valitsus.ee/sites/default/files/content-editors/arengukavad/vagivalla_ennetamise_strateegia_2015-2020_kodulehele.pdf> (09.08.2017).

Kaugia, S. "Õigusteadvuse olemus ja arengudeterminandid" (2011) (Essence of Legal Consciousness and Determinants of Development).

Koolieelse lasteasutuse riiklik õppekava. – RT I 2008, 23, 152.

Laps perevägivalla ohvrina. <http://abiksohvrile.just.ee/et/lapsele/laps-perev%C3%A4givalla-ohvrina> (25.09.2017).

Märja, T. "Euroopa Liidu hariduspoliitika mõjutused Eestis" – *Eesti ja Soome haridus ning muutused EL-i hariduspoliitikas 1990-2000. Artiklite kogumik*. L. Jõgi, T. Jääger, R. Leppänen, R. Rinne (Koost). (2008).

Narits, R., Kaugia, S., Pettai, I. "The Significance of Recognising Domestic Violance, in Light of Estonian Legal Experts´ Opinion and the Prospects for Systematising the Relevant Legislation" – *Juridica International* 24, 2016, pp 128-138.

Pettai, I., Kaugia, S., Narits, R. "Perevägivald nõuab jõulisemat juriidilist sekkumist" – *Riigikogu Toimetised*, 31, 2015, lk 155-167.

Pettai, I., Narits, R., Kaugia, S. "Of the Current State and Outlook of the Legal Regulation on Domestic Violence Based on the Results of an Expert Poll Carried Out Among the Estonian Legal Practitioners"– IX, *Juridica* (2015), pg 645-658.

Pettai, I., Narits, R., Kaugia, S. "Perevägivalla juriidilise regulatsiooni hetkeseis ja perspektiiv Eesti õiguspraktikute küsitluse põhjal" – *Juridica*, IX, 2015, lk 645-658.

Risnoveanu, A. "The Students' Socialization – A Real and Actual Challenge for the School Organization" – *Journal of Educational Sciences & Psychology*, LXII, No 1B/2010, p 73.

Seletuskiri gümnaasiumi riikliku õppekava määruse eelnõu juurde. 05.01.2010, pg 37, 39 (Explanatory note to the draft regulation of upper secondary school curriculum.) (in Estonian) <https://www.hm.ee/sites/default/files/2010._aasta_pohikooli_oppekava_seletuskiri.pdf> (10.08.2017).

Sotsiaalministeerium. "Eesti elanikkonna teadlikkuse uuring soopõhise vägivalla ja inimkaubanduse valdkonnas. Uuringu aruanne". TNS EMOR (2014). (The Ministry of Social Affairs. Attitudes of Estonian inhabitants in relation to gender-based violence and human trafficking. Survey report.) (in Estonian) <https://www.sm.ee/sites/default/files/content-editors/eesmargid_ja_tegevused/Norra_toetused/Koduse_ja_soopohise_vagivalla_vahendamise_programm/elanike_hoiakud_soopohise_vagivalla_ja_inimkaubanduse_valdkonnas2014_aruanne_tns_emor_loplik.pdf> (10.08.2017).

Tartu Kristjan Jaak Petersoni Gümnaasiumi õppekava (The Curriculum of Tartu Kristja Jaak Peterson Gymnasium) (2016).

< https://kjpg.tartu.ee/img/image/Dokumendid/KJPG_oppekava_20161.pdf> (25.09.2017).

AUGGMED: DEVELOPING MULTIPLAYER SERIOUS GAMES TECHNOLOGY TO ENHANCE FIRST RESPONDER TRAINING

Jonathan Saunders, MSc
CENTRIC (Centre of Excellence in Terrorism, Resilience, Intelligence and Organised Crime Research), Sheffield Hallam University, UK
Researcher

Helen Gibson, PhD
CENTRIC, Sheffield Hallam University, UK
Lecturer in Computing

Roxanne Leitao, MSc
CENTRIC, Sheffield Hallam University, UK, Researcher;
University of the Arts, London, UK

Babak Akhgar, PhD
CENTRIC, Sheffield Hallam University, UK
Director of CENTRIC, Professor of Informatics

Keywords: serious game, training, virtual reality, simulation, AUGGMED, Exodus

ABSTRACT

Many serious games are designed for single player access only. However, the benefits of the immersive nature of serious games and virtual reality may be enhanced when teams who usually train together can also do so within a virtual environment. The purpose of this article is to outline the architecture of the AUGGMED serious game and discuss the technical challenges faced when creating a multiplayer counter terrorism training serious game utilising virtual reality, touch screen interfaces and a realistic crowd simulation. AUGGMED is designed using an agile modular approach utilising user centred design principles, with each technical developer owning a set of tools which are continuously integrated, piloted, and improved throughout the development cycle. Constant piloting with first responders enables iterative improvements, which meet end user training requirements. Building a multiplayer training game specialised in providing realistic simulation of real situations, and enabling users to interface with the simulation through virtual reality identifies a large set of technical challenges. The article identifies a number of the challenges faced while developing AUGGMED and the solutions used to overcome them, including barriers and logistical/technical difficulties to integrating multiple existing (Exodus crowd simulation) and new (virtual reality) technologies into a single serious game for training first responders.

INTRODUCTION

With the ever-changing security threat landscape, the rapid advance of technology, and the need for more advanced and realistic forms of training, modern organisations are looking for novel, state of the art solutions to prepare for terrorist and organised crime threats. Alongside traditional physical dangers posed by terrorists and extremists, a new threat has emerged in recent years: cyber-attacks. As the line between on - and off-line crime blurs, targeted attacks such as denial of service and ransomware, which can be designed to extort money and information (Veerasamy, Grobler and Von Solms, 2007; Broadhurst et al., 2014), can also be used to cripple critical infrastructure (Miller and Rowe, 2012). Cyber-attacks delivered in conjunction with traditional physical attacks aim to maximise impact and hamper response efforts (Leyden, 2008) Thus any training platform targeting the response to such threats should take into account the cyber-element from a high-level training point-of-view.

Traditionally, training for mitigating against these threats may include a combination of desk-based, table-top and live exercise scenarios requiring the investment of significant resources (financial and human), time and effort (Allen, 1992) as well as lacking replicability and standardisation. These traditional forms of training also often require trainees to be co-located increasing the financial and logistical costs. Finding methods of training which can reduce the resource requirements, geographic limitations, and investment for both small and large scale training scenarios would enable trainees to develop skills and experience, which could be used in a far greater number of situations. The AUGGMED project aims to alleviate these considerations through the development of a serious game which encompasses elements of augmented and virtual reality, but can also be played on standard desktop and mobile devices as required. Furthermore, AUGGMED aims to provide a solution which incorporates multiplayer access enabling remote teams to train together even when they are geographically spread. In order to develop such a solution, additional architectural considerations must be factored in to the design which can keep track of the movements and actions of each player as

well as how this affects others experiencing the simulation in the same exercise.

A serious game is defined as 'any piece of software that merges a non-entertaining purpose (serious) with a video game structure (game)' (Djaouti, Alvarez and Jessel, 2011). Serious games have been found to have impacts on the player which can be affective and motivational, facilitate behaviour change, enhance knowledge acquisition and understanding, improve motor skills, have perceptual and cognitive benefits, physiological benefits, and improves social and other soft skills (Connolly et al., 2012). Concerning AUGGMED, serious games have already been shown to improve triage accuracy (Knight et al, 2010) [an intended pilot scenario] whilst the military already have a long history in the use of simulation and serious games (Smith, 2010) which may provide cross-overs into aspects of counterterrorism training.

This paper will introduce the goals and aims of the AUGGMED project, the underlying envisioned architecture and implementation methodology, the challenges faced during the initial phases of development, the solutions to those challenges and the remaining considerations for forthcoming piloting scenarios.

1. THE VISION FOR AUGGMED

The AUGGMED (Multi-agent counter terrorist training in mixed reality environments with an automated serious game scenario generator) project is designed to enable law enforcement agencies (LEAs), paramedics, firefighters and other first responders to train simultaneously in a single virtual environment. The environment represents real world locations populated with realistic, civilian agents who react and respond to events, other trainees and threats. Using modern games and server technology the AUGGMED platform enables users to train from any physical location, allowing multiple organisations to collaborate on training without the requirement of co-locating the trainees.

The project has completed one of three pilots which will be carried out throughout development in twelve month intervals. These have already proven to give both trainers and trainees opportunities and capabilities which would not be possible in real world exercises.

The AUGGMED platform, as shown in Figure 1, provides a single system in which both trainers and trainees can operate in the same environment. The trainees access the platform through a range of devices (mobile, tablet, desktop PC, laptop, virtual reality headsets and haptic vests) while the trainers controlling the overall definition and progression of the scenario also have access to live analytics for feedback and evaluation. The AUGGMED project itself centres on three main scenarios, an airport terror attack and fire scenario, an underground station hot bag and explosion scenario and a combined cyber/terror attack on a busy port. These are realised through technological components including the Unity games engine, communications layer and simulation layer.

Upon completion, utilising the platform would enable organisations to significantly reduce the resource requirements of training for large scale events, such as terrorist attacks and organised crime threats (Allen, 1997). Alongside this it would enable trainers to tailor training specifically to the trainee's requirements using a set of trainer tools. These enable the trainer to customise variables such as time, location, population, demographics, trainee capabilities and threat objectives.

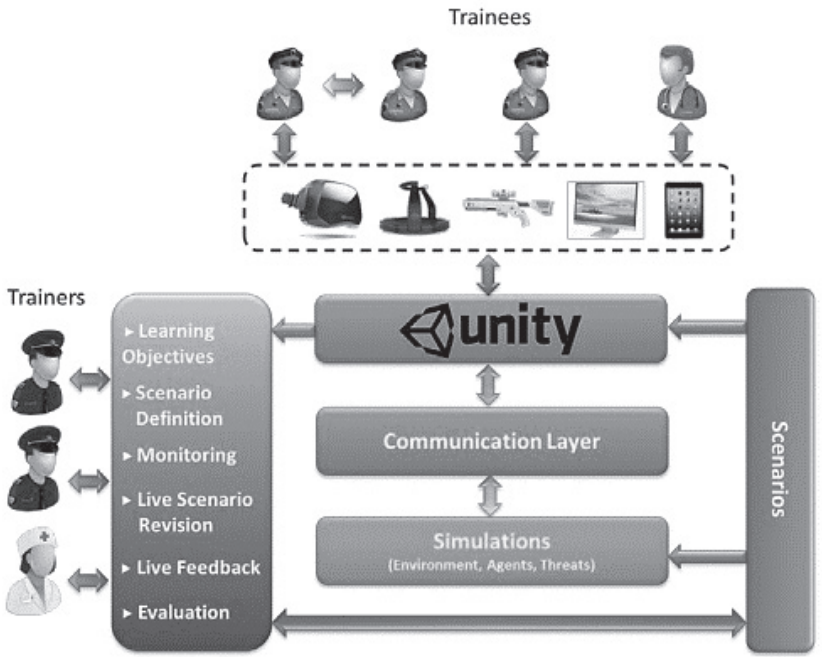


FIGURE 1: AUGGMED PLATFORM

The system incorporates realistic fire and explosion simulations which enable trainees to experience complex life threatening situations, which would not be possible in real world training environment using Exodus. These simulations assess and calculate the impact of these events on both civilians and trainees, realistically replicating the outcomes of smoke inhalation and injuries through negative effects on the trainee avatars.

The AUGGMED platform can be utilised on touch screen devices, standard PC's and in virtual reality, allowing end users to train using the most appropriate input method for their requirement. Each input method is designed to enable trainees to be able to meet their training requirements depending on the context of the scenario they are using.

Using virtual reality enables trainees to build upon both their technical and decision making skills as well as developing their emotional resilience to stressful and often psychologically difficult events (Wiederhold and Wiederhold, 2008). The capability to develop the emotional resilience of

first responders is a unique aspect to virtual reality training when compared to standard training methods. Alongside this the system will feature a full immersion mode utilising a virtual reality treadmill, gun controller and haptic feedback vest capable of simulating heat, gunshots and touch. These systems will combine to provide a fully immersive training experience for trainees, further enhancing their training experience and better enabling them to reach their learning objectives.

1.1 AUGGMED ARCHITECTURE OVERVIEW

The AUGGMED platform is comprised of a set of core systems, the platform itself utilises the Unity® Games Engine to handle the base game algorithms responsible for rendering, physics simulation, sound, and networking. The trainer tools are built on top of this, which will enable trainers and trainees to customise, observe, record, analyse and assess any training scenario and trainees on an individual basis. Civilian intelligence, fire and explosive simulations are processed and handled by the Exodus platform, a civilian population simulation program designed for large scale evacuation models.

The architecture of AUGGMED consists of a number of individual components, each responsible for a specific aspect of the platform. Figure 2 displays the individual components contained within the AUGGMED system that interact and integrate with one another.

This section introduces each of the components within the AUGGMED system, discusses the motivations for their inclusion while presenting their roles and functionalities in the context of what the AUGGMED platform is aiming to achieve. This section lays the groundwork for the review of the technical challenges faced when developing the system shown in Sections 2 and 3.

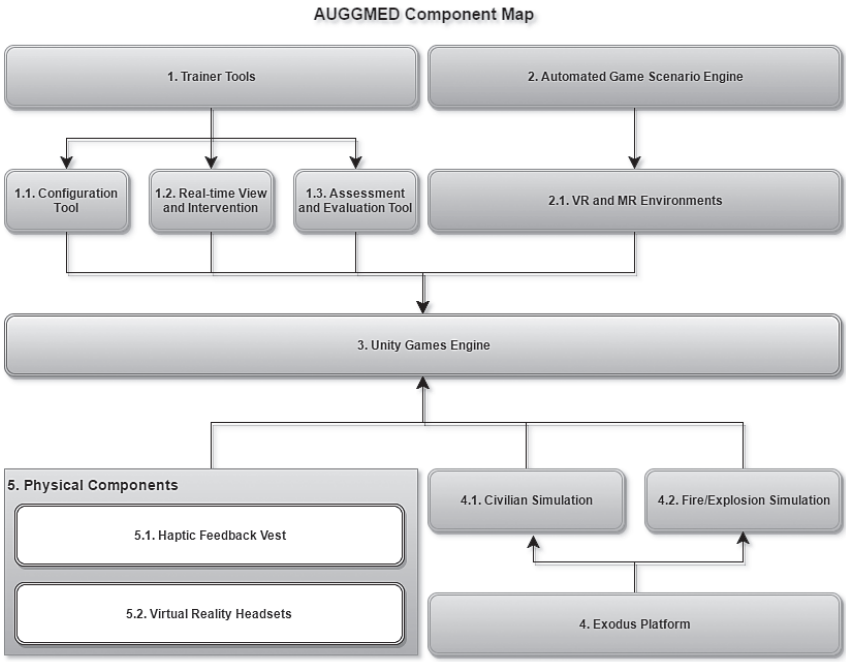


FIGURE 2: COMPONENT VIEW OF AUGGMED

1.2 THE TRAINER TOOLS

To be able to control the simulation and provide benefits to the trainer as well as the trainees, AUGGMED features a 'trainer tools' interface and associated functionalities which give each trainer fine-grained control over how the scenario evolves. The trainer tools consist of three individual components, each of which is designed to enable trainers to maximise their capabilities whilst using the platform. The trainer tools have been designed based on Microsoft's design layout for Windows 10 devices . This ensures interaction with the trainer tools is consistent with the operating system and retains a specific theme on both desktop personal computers and touch screen devices (such as the Microsoft Surface). The trainer tools themselves are then divided into three further components: the configuration tool, real-time view and intervention interface, and the assessment and evaluation tool.

1.2.1 Configuration Tool

The configuration tool enables trainers to generate unique and customised training scenarios by changing setup variables such as time, location, population, potential cyber-attacks, trainee roles and capabilities, and the severity of the threat they face. This is achieved by creating a custom scenario which can be saved and re-used at a later date. Each scenario can contain a set of roles, each role uses an inventory system to determine the capabilities of the trainees who are performing that role. The interface for setting up such a scenario is displayed in Figure 3, while the character selection interface is shown in Figure 4.

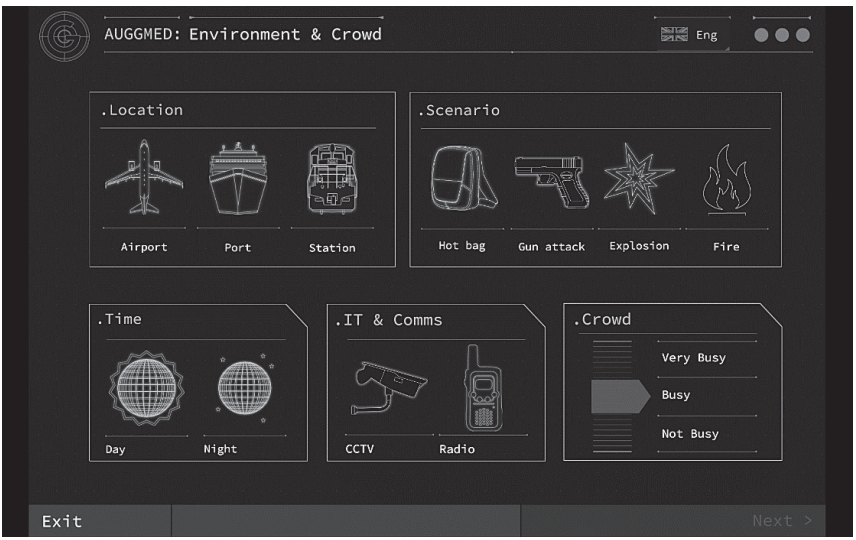


FIGURE 3: AUGGMED CONFIGURATION INTERFACE

Trainers can build a list of template inventories allowing them to quickly change the items available depending on the requirements of the training scenario. An individual trainee can carry up to five items depending on the type of objects they require. A role has one primary item slot, used for large items such as rifles, extinguishers or fire axes; one secondary slot for small items such as pistols, triage tags or a torch; and three utility slots for carrying utility items such as explosive devices, bomb disposal kits, or gas masks.

FIGURE 4: AUGGMED CHARACTER CONFIGURATION

1.2.2 Real-time View and Intervention

The real-time view and intervention tool enables trainers to observe trainees from a number of perspectives and intervene when necessary. Trainers can observe the entire simulation from a bird's eye perspective and watch an individual or group of trainees, simultaneously through the zoom controls. They can also set the camera into a "follow" state which automatically tracks and focuses in on the movements of the selected trainee.

Trainers can also switch to "player perspective" allowing them to experience exactly what an individual trainee sees and hears during the exercise. When a scenario begins, a trainer uses this tool to deploy individual trainees and threats to any selected location in the environment. Similarly, if a trainee is shot and killed they can be re-deployed by a trainer, if it is required, to achieve the learning objectives of the scenario. Trainers also select if a fire will be included in the scenario and where in the environment it will begin. At anytime during a simulation the trainer can initiate a pre-selected cyber-attack, these include loss of CCTV and/or radio communication interference.

In addition to trainers, observers are also able to use some of the functionality of this tool to monitor the progress of trainees, however they do not have access to the intervention aspects such as deployment, fire initialisation or cyber threat controls.

1.2.3 Assessment and Evaluation Tool

The assessment and evaluation tool collects and analyses statistical data about the performance of individuals and groups of trainees. It then collates and outputs this data as a report for trainers and in a visual format immediately after a scenario has concluded. It records metadata for the entire scenario, allowing trainers to replay the scenario and re-observe trainee behaviour, actions and decisions as if it were a live scenario.

The data collected includes statistical information regarding player actions such as bullets shot, enemies hit, civilians hit, and visual data such as movement heat maps. Trainers will be able to use this data to support them during debriefing sessions and as inputs into future training scenarios. Trainees' will have access to a subset of the data relating to their own personal performance at the conclusion of an exercise.

Due to the multiplayer element of AUGGMED, an interesting use case for the statistical tracking data is the possibility to compare team and individual performances. Furthermore, it is not always clear what might represent a successful individual performance as many members of SWAT or counterterrorism teams may play more of a tactical role, which may not translate well into 'good statistics'.

1.3 AUTOMATED GAME SCENARIO ENGINE

The Automated Game Scenario Engine manages the location, environmental factors and interact-able objects. This engine ensures that the scenarios developed are non-deterministic and that even if a trainee re-enters the game at the same location with the same general theme (e.g., terrorist attack) the area in which the attack begins, the reactions of the civilians, and the extent to which smoke or exit routes can cause

problems can all be modified. Monitoring of how the scenario is initialised can then be combined with player behaviour to identify where training efforts may need to be focused.

1.3.1 VR and MR Environments

The Virtual Reality (VR) and Mixed Reality (MR) environments within the AUGGMED platform dictate the virtual geometry, environmental behaviour and available fire locations. Each location has a number of preselected locations for a fire to begin as well as varying the size and types of fire available for trainers to use. Each location is unique and provides opportunities for first responders to train in an environment which represents a real world location.

1.3.2 AUGGMED Scenarios

A part of the automated game scenario engine is the individual scenarios which are simulated within the AUGGMED platform. There are multiple scenarios per location including terror attack, hot bag, explosion and fire. Each type of scenario changes the capabilities of the trainees and allows for additional elements to be set up before a scenario begins, for instance choosing the location of a fire or placing suspicious items into the scenario.

1.4 UNITY GAMES ENGINE

Unity® is a multi-platform games engine enabling developers to rapidly develop and deploy software on a multitude of platforms simultaneously. Games engines are software frameworks which facilitate the creation and development of games by providing a base set of functionalities and capabilities, such as rendering, audio and physics calculations (Unity Technologies, 2016).

The Unity engine acts as the core of the AUGGMED project, handling a large set of the backend features and requirements of the system. As well

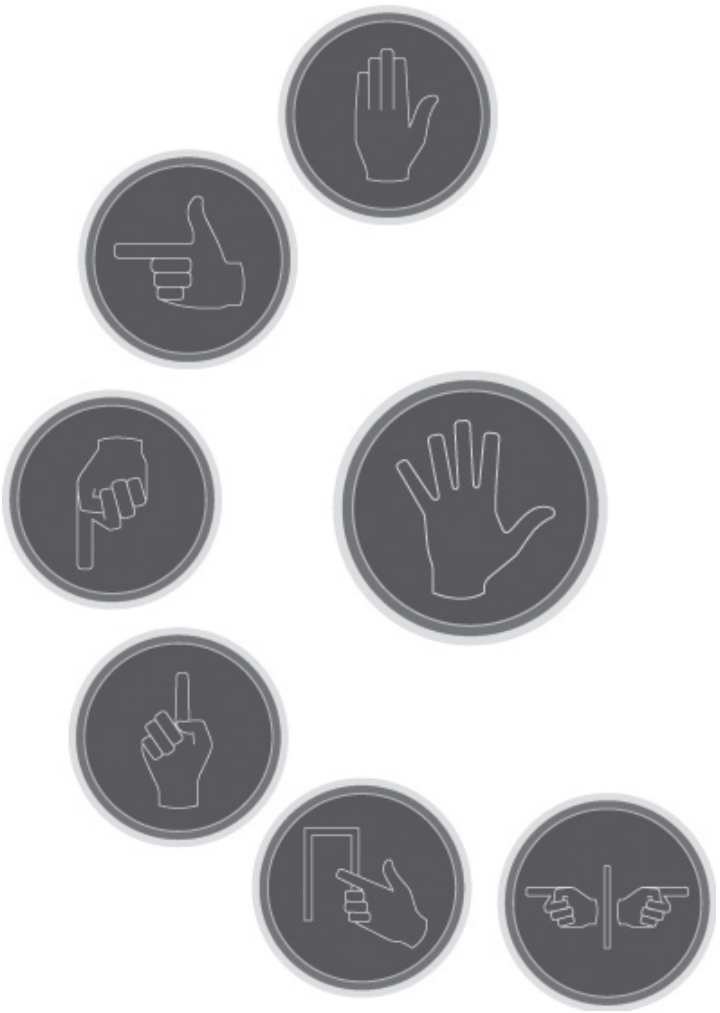


FIGURE 5: CIVILIAN COMMAND ICONS

as managing the rendering, audio and physics it also provides built in networking capabilities which enable AUGGMED to create servers and clients, which connect to these servers. Unity handles the entire visual, audial, interface and communications within the AUGGMED platform, all other components communicate through and/or are realised using the game engine.

As part of the rendering system for AUGGMED, all the main components for the trainees heads up display (HUD) are represented using Unity's built in 2D rendering canvas system. This system, which has been built specifically for developers to create player interfaces, enables the AUGGMED project to create dynamic and intuitive control systems for the trainees to use. An example of this is the player to civilian interaction inputs, a trainee can issue commands such as "Get Down" and "Stop" to civilians inside a training scenario at any time. For standard keyboard inputs this can be achieved through keyboard commands, however when using a touch screen device the player will require touch specific methods of initiating commands to players. Figure 5 displays the touch screen gesture control inputs available to a trainee, the central button represented by an open palm is used to reveal and hide the surrounding controls. These controls then directly map to a single command a trainee can give to civilians, these include: stop, move, get down, get up, evacuate now and get out of the way.

1.5 EXODUS PLATFORM

The Exodus platform is a civilian simulation system which realistically replicates civilian behaviour during an evacuation event. It also simulates behaviour relating to commands from first responders as well as injuries and fatalities due to fire and explosions (Galea, Owen and Lawrence, 1996).

1.5.1 Civilian Simulation

The civilian simulation system is responsible for realistically replicating civilian behaviour during a scenario, based on real world data it replicates civilian movements, reactions and injuries throughout a scenario. The number of civilians in any given scenario can range from tens to high hundreds depending on the requirements of the trainer.

The Exodus platform calculates all civilian information before sending that information to the Unity Engine. The engine then updates all of the relevant information on the server, and all local clients, before sending

contextual information back to exodus, such as player movements and actions.

1.5.2 Fire and Explosion Simulation

The Exodus fire and explosion simulations are responsible for calculating and producing data which create realistic representations of these events in the environment provided. In the case of a fire, this includes the build-up of smoke, the effect of inhalation of the smoke on players and civilians, and the spread of fire throughout a given location. The explosion simulation handles information relating to an explosives area of influence, depending on the type and amount of material used. This information is built up using a predictive algorithm which determines the effect of an explosion on an actor including fatalities and injuries.

1.6 PHYSICAL COMPONENTS

The AUGGMED platform relies on a selection of specialised physical components to deliver the fully immersive virtual reality experience. Whilst not required for all users of AUGGMED, these components enable trainee's to experience a significantly more interactive scenario through the use of virtual reality headsets and haptic feedback vests.

1.6.1 Haptic Feedback Vest

The vest provides new methods for providing nonstandard information to a trainee through the use of a number of built in components, which can replicate temperature change and kinetic feedback. The vest will react to the state of the player character in the virtual environment and will convey specific information such as being shot, walking too close to a heat source or a tap on the shoulder. Combined with the virtual headset, this will give the AUGGMED platform an effective way of portraying non-visual or audial information, enabling trainees to make better informed decisions as their experience ever more closely resembles the real world environment.

1.6.2 Virtual Reality Headsets

The virtual reality headsets which interface with AUGGMED will provide trainees with an immersive method of engaging with the platform. Modern headsets not only display the environment in 3D, they allow 360 degrees of rotation and can track real world movements.

With the recent release of commercial virtual reality headsets they have become far more affordable and reliable. Both the HTC Vive[1] and Oculus Rift[2] provide accurate head-tracking and high quality visual fidelity. Users training using virtual reality will require state-of-the-art computers with powerful rendering technology when compared to standard desktop and touch screen computer.

Virtual Reality users will also be able to use other specialised input devices for their training including replica gun controllers and virtual reality treadmills, such as the Virtuix Omni.[3] These combined with the haptic feedback vest being developed have the potential to maximise the levels of interaction and immersion. Higher levels of immersion have been found to improve learning of geospatial tasks, including search operations and environmental awareness (Pausch, Proffitt, and Williams, 1997).

1 https://www.htcvive.com/

2 https://www.oculus.com/

3 http://www.virtuix.com/

2. DEVELOPMENT APPROACH

The AUGGMED project follows an agile user-centred design methodology focused on attaining constant end user input and integrating the results with future developments of the platform.

> *'Agile development excels in exploratory problem domains — extreme, complex, high-change projects — and operates best in a people centered, collaborative, organizational culture.' (Cockburn and Highsmith, 2001).*

Agile's focus on rapid iteration and approaching the development process from the bottom up fits precisely with the aims of the AUGGMED project. Through the identification of non-rigid development targets and milestones the platform can focus on developing the highest priority features and easily react to changing priorities during development.

The design methodology followed by AUGGMED utilises an approach of compartmentalising elements of the platform into independent modules assigned to individual technical partners. These modules encompass a specific technical requirement of the project, such as environments, and ensure a single, accountable point of responsibility exists. Each module owner is responsible for developing, testing and integrating their work into the core project, with the technical lead responsible for overseeing the integration process, ensuring AUGGMED remains stable, responsive and reliable.

2.1 DEVELOPMENT

Development of the individual modules of the AUGGMED platform started once an initial set of end user requirements was gathered. These were collated with the help of LEAs and other blue light services who usually participate in table-top and live exercises. These requirements shaped the core mechanics of the game and helped the developers prioritise features based on their capability to help trainees meet learning

objectives. Following the requirements gathering phase of the project, the outputs were consolidated and prioritised based on the resource requirements of each individual feature weighted against the end users own promised requirements.

Using this method deadlines were set out for the systems which were required for the first pilot of the platform. Subsequent features and their deadlines were introduced based on observations, feedback, and more requirements identified during the first pilot. This iterative method of requirements gathering and feature prioritisation has enabled the developers and end users to build the AUGGMED platform to client specifications without significant redundancies in work.

This iterative approach which is at the core of agile software development methodologies ensures the project can continuously adapt to end user requirements and promotes the need to constantly integrate, test and pilot the software. This in turn ensures the AUGGMED serious game is bug free, reliable and robust.

2.2 TESTING

New features and large changes to the core of the AUGGMED platform are developed and worked on in separate independent branches of the project for a maximum of two weeks. Before integration into the main branch at completion of the feature the entire branch must be rigorously tested for errors, processing and rendering speeds, and network behaviour, as well as code and project continuity.

Upon passing the testing process the feature is merged into the core project and re-tested to ensure no merge conflicts interfered with the process of merging the two versions of the platform. Failing either of these tests requires the technical developer to address the issues found and restart the testing and merging process.

Following this method of internal testing, both before and after integration takes place, ensures any potential problems can be identified and addressed as early as possible in the development process.

2.3 INTEGRATION

Integration of every module of the AUGGMED platform is handled using GIT version control software[4] and third party merge conflict management tools[5]. The principal technical developer in charge of a specific module is responsible for carrying out the merge, resolving any conflicts arising during the process and testing the full integration. Every module, task and subtask being developed in a development cycle is discussed during bi-weekly development meetings to ensure all technical developers are aware of coming changes; this reduces the chances of significant merge conflicts and duplicate work being carried out.

The integration of the separate modules is overseen by the lead technical developer, who handles any significant feature merges or conflicts. This certifies continuity of the merged content and ensures the lead technical developer understands the purpose, implementation and behaviour of each module.

2.4 PILOTING

Piloting is a critical aspect of the AUGGMED development process, it is not only responsible for acquiring a refined set of user requirements, it also serves as a method of disseminating the progress of the project and stress testing the capabilities of the platform.

The critical nature of the piloting process in regard to future development of the platform creates a definitive set of deadlines and milestones which must be adhered to throughout the project. It also ensures the development of the platform is grounded through end user inputs, testing and feedback.

Each pilot is designed to test the entirety of the core AUGGMED serious game alongside a specific input method. The purpose of the first pilot was to test the mouse and keyboard control system for both the

[4] https://git-scm.com/

[5] https://sourcegear.com/diffmerge/

trainers and trainees alongside the core functionalities required for all training scenarios. These core functionalities include network stability, system reliability, agent behaviour, hardware load and avatar interaction capabilities.

The second pilot will once again stress test these core functionalities alongside the mouse/keyboard control method. In addition to these features, the second pilot is also required to test the virtual reality capabilities of the system. This includes an assessment of the ability of end users to adopt virtual reality as an input method - which is likely to be alien to most users - and compare its effectiveness against standard inputs.

The third pilot will introduce the mixed reality implementation of the AUGGMED platform with users training simultaneously within the same space using standard PC's, virtual reality and augmented reality. This final pilot will validate the use of multiple novel control systems and technologies, which have yet to be used within modern serious game systems.

3. TECHNICAL CHALLENGES

Thus far, the AUGGMED platform has overcome a number of significant technical challenges throughout its development, leading up to, and beyond the first pilot. These challenges both guided and defined the outcome of the platform including its simulation capabilities, concurrent users and customisability.

3.1 MULTIPLAYER NETWORK SYNCHRONISATION

A key challenge faced by the project was the amount of network capacity required for each client and by the server hosting a scenario.

A scenario could have 200 to 800 civilian agents at any one time. Exodus would simulate the origin and targets of each agent, and send an update to the Unity games engine every 10^{th} of a second. This update contained positional information for every agent. Within the games engine each agent's movement delta was calculated between the last and next position and a vector, with both direction and magnitude, and could therefore be used to interpolate agent positions. This information would be used to simulate movement of the agents on the server and would be relayed to all clients.

Given the number of civilian agents, the amount of information sent between the server and individual clients has to be optimised at every opportunity, for this reason all orientation specific information was omitted from the synchronisation process of artificial intelligence agents, and would instead be inferred by calculating the vector between the origin and the target of an individual agent. Whilst rotational data is insignificant for an individual agent, it becomes a considerable task to send the rotational data of hundreds of agents multiple times per second.

A player's position, look rotation, and body rotation, data was synchronised alongside agent data. Rotational data was included in the synchronisation process for players to ensure identical player behaviour was

replicated between all clients. Whilst this meant more information was synchronised for a player compared to an agent, the small number of concurrent players ensures it is not a significant load for the network system. The total data, required to synchronise players per update is the sum of these variables and whilst insignificant compared to the collective agents data requirements, adds to the total network requirements of AUGGMED. The equation shows how to roughly calculate the total server network load required based on the number of players, while Table 1 shows the amount of data transmitted for each element of position data for each player.

TABLE 1: NETWORK REQUIREMENTS FOR TRANSMITTING PLAYER DATA

Variable	Type	Size	Variable
Player Position	Vector 3	12 (4+4+4)	*p*
Body Rotation	Quaternion	16 (4+4+4+4)	*b*
Look Rotation	Quaternion	16 (4+4+4+4)	*l*
Total Size Per Player	44 Bytes		

$$D \cong \sum_{i=0}^{n} u(p + L + b)$$

As an example, a single server simulating 400 agents with a single client connected would be sending a total of around 26,000 bytes per second based on the standard variables used to control each agent. This is based on a single agent's data containing a single (single-precision floating-point) value for time; two single values for origin position; two single values for target positions; an integer representing the character's stance; and these values being updated three times per second between the server and client. The relationship between these components is shown in Equation (2), while Table 2 shows the requirement for each individual agent.

TABLE 2: AGENT DATA REQUIREMENTS

Variable	Type	Size	Variable
Time	Single	4	
Agent Position	Vector 2	8 (4+4)	
Agent Target	Vector 2	8 (4+4)	
Stance	Integer	2	
Total Size Per Agent	22 Bytes		

$$A = t + o + T + s$$

A standard simulation could contain around five trainees, three red team players, three observers and a second trainer. Assuming a simulation contains four hundred agents being synchronised between users three times per second (u). Equation (3) defines the equation required to calculate the amount of bytes per second needed for an individual user, and Equation (4) shows the final method of calculating the rough bandwidth requirement to send the information to all clients effectively.

$$U \cong \sum_{i=0}^{n} uA$$

To discover the total expected bandwidth requirement of the server, the total number of concurrent users must be calculated, which in the above example is roughly equal to 344,256 bytes per second, or 344.3Kbps.

$$B \cong cU$$

The method for calculating the entire bandwidth required for the server to effectively manage the network traffic of the AUGGMED platform, as shown in Equation (5) was defined by the methods used during the design process of AUGGMEDS network capabilities.

$$B \cong c\left(\sum_{i=0}^{n} u\left(\sum(t, o, T, s)\right)\right) + \mathrm{D}$$

This total bandwidth requirement does not cater for all other messaging systems required to enable player interaction with the system, such as player voice commands.

Due to the amount of information the server is expected to send and receive, developing efficient and minimal methods of updating each client's individual game state was a core challenge the development team would need to overcome.

During the course of the first pilot test of the platform it was discovered that the built in network system UNET[6], which is Unity's standard network API, struggled to handle the level of data and network connections required by the platform. This resulted in an unreliable network with synchronisation problems and inconsistent agent behaviour. As a result of this the developers decided to look for alternative network API's, such as Photon[7], which would be better suited to handle the amount of data and concurrent users required by AUGGMED. Whilst this decision would set back development, the requirement for a stable and scalable network API far outweighed the importance of other features planned in development. This decision meant a re-prioritisation of work and new targets and milestones were defined.

3.2 MULTI-MODAL PLAYER INTERACTIONS

A core aspect of the AUGGMED platform is the capability for users to train using their preferred method, which can enable them to better meet their learning requirements, style and availability. This includes the ability to train using a standard mouse and keyboard setup, using a touchscreen device or utilising virtual reality headsets. These interaction methods require specific considerations when it comes to player input systems, the on-screen heads-up display (HUD) and their methods of interacting with the environment.

6 https://docs.unity3d.com/Manual/UNetOverview.html

7 https://www.photonengine.com/en-US/Photon

McMahan et al. (2012) have shown that input methods used to interact with a virtual environment can have a significant effect on the performance output of the user. This difference in performance can make it difficult for a trainer to fairly evaluate multiple trainees using different interaction methods while performing the same task. Identifying the strengths and weaknesses of these methods and building upon these is critical in helping trainees' achieve their learning requirements.

Alongside different interactions, players using a selection of devices will require diverse levels of information displayed depending on their capability. An example of this is a touch screen user verses a standard desktop user. Players controlling their avatar using a mouse and keyboard are presented with standard controls attributed to first person shooter (FPS) games as well as an on screen crosshair, whereas a touch screen user needs to see their controls on screen as well as the crosshair.

Table 3 displays the current and planned control systems for each input method, these are based on current best practices and successful serious and standard game controls.

TABLE 3: MULTI-MODAL CONTROLS

Interaction Method	Movement Control	Look Control	Jump/Sprint/ Crouch	Civilian Interactions
Mouse/ Keyboard (Current)	W, A, S, D Keyboard Keys	Mouse Movement	Spacebar, Shift, CTRL	Keyboard Number Keys
Touch Screen (Current)	Radial Joypad Control	Radial Joypad Control	Jump Button, Sprint Toggle, Crouch Toggle	Interaction Buttons
Virtual Reality (Planned)	Controller Joypad	Head Rotation	Controller Buttons: A, Left Joypad Press, B	Radial Selection

These control systems were based on tried and tested methods utilised by standard computer games on personal computers and touch screen devices.

The largest challenge when developing a multimodal serious game is to give all players the same capability, regardless of their device. To

overcome this, it was decided to accept the strengths and weaknesses of each interaction method and build upon these to cater them to specific areas of training.

Standard desktop interaction using a mouse and keyboard allows for the most balanced form of training and the most precise control methods (McMahan et al, 2012). Whilst it loses virtual reality's geospatial and emotional benefits; it has lower resource requirements, is more accessible for trainees, and is easier for remote training. This standard form of input provides greater precision capabilities to trainees and is the most accessible of the three interaction methods.

Touch screen device interactions enable even more capabilities for remote training; most touch screen devices are portable enabling for trainees to use AUGGMED on the move and can further reduce the resource cost of training. However these benefits are offset by the loss in precision which a mouse and keyboard can give, and virtual reality's emotional resilience and geospatial capabilities. Training using touch screen devices is the cheapest and most portable of the three interaction methods, enabling remote training capabilities and cost effective training solutions.

Virtual Reality can provide the most immersive experience and is capable of greater emotional resilience training (Wiederhold and Widerhold, 2008) and development of geospatial skills (Pauch, Proffitt and Williams, 1997; Bowman and McMahan, 2007) which are often overlooked in traditional forms of training. However these benefits have greater costs and less portability due to the higher technical requirements of virtual reality and the necessity for more hardware. Virtual reality training delivers the most complete training experience, capable of developing a multitude of skills from situational awareness, geospatial capabilities, tactics, to communication and stress management.

Through the identification of the strengths and weaknesses of each interaction method the AUGGMED platform can ensure greater knowledge transfer through specific devices by targeting the capabilities of each device to better support its strengths. For instance mouse and keyboard users aiming and controls are finely tuned to allow effective and realistic movement within the simulation without the loss of the fine controls associated with using a mouse.

Using this method we identified the best forms of interaction for both trainers and trainees. Whilst it was decided all devices could promote learning for the trainees, the trainers only required the capability to customise, observe and intervene with a scenario accurately and efficiently. With this in mind only mouse and keyboard input was implemented for the trainers.

CONCLUSION

The AUGGMED project identified and overcame a number of technical challenges during the first year of development. These challenges introduced important questions to the development process utilised during the project and the solutions implemented also require reflection.

The challenge of creating a multiplayer serious game which contains tens of players and hundreds of intelligent agents' highlighted limitations of Unity's built in UNET network protocol, and of standard Wi-Fi connections and hardware. The discovery of these problems during development and during the first pilot project highlighted the necessity for constant testing, piloting and refinement during the development process. Utilising the findings of the first pilot, the development process of the platform was changed, with more emphasis on early testing of core systems. Through this process alternative networking API's were identified as potential replacements to UNET which are better suited to AUGGMED's networking requirements.

Similarly the multi-modal input challenges faced by the project reinforced the requirement for informed development planning, research and end user feedback. Through efficient and effective planning during development, the AUGGMED platform built upon the strengths of using multiple input methods to ensure the platform can deliver a complete training experience, regardless of the devices used to achieve the learning requirements.

Leading up to the second pilot of the AUGGMED serious game, learning from these challenges and implementing the changes to the development process has reinforced the ideal that efficient planning and development alongside end users can help overcome significant barriers when developing new technologies.

ACKNOWLEDGEMENTS

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 653590.

Contacts:

Jonathan Saunders
CENTRIC
Sheffield Hallam University, UK
E-mail: jonathan.saunders@shu.ac.uk

Helen Gibson
CENTRIC
Sheffield Hallam University, UK
E-mail: h.gibson@shu.ac.uk

Roxanne Leitao
CENTRIC
Sheffield Hallam University, UK;
University of the Arts, London, UK
E-mail: r.leitao@shu.ac.uk

Babak Akhgar
CENTRIC
Sheffield Hallam University, UK
E-mail: b.akhgar@shu.ac.uk

REFERENCES AND SOURCES

Allen, P., 1992. *Simulation Support of Large-Scale Exercises: A REFORGER Case Study, RAND*. R-4156-A.

Bowman, D.A. and McMahan, R.P., 2007. Virtual reality: how much immersion is enough?. *Computer*, *40*(7).

Broadhurst, R., Grabosky, P., Alazab, M. and Chon, S., 2014. Organizations and Cyber crime: An Analysis of the Nature of Groups engaged in Cyber Crime. *International Journal of Cyber Criminology*, *8*(1).

Cockburn, A. and Highsmith, J., 2001. Agile software development, the people factor. *Computer*, *34*(11), pp.131-133.

Connolly, T.M., Boyle, E.A., MacArthur, E., Hainey, T. and Boyle, J.M., 2012. A systematic literature review of empirical evidence on computer games and serious games. *Computers & Education*, *59*(2), pp.661-686.

Djaouti, D., Alvarez, J. and Jessel, J.P., 2011. Classifying serious games: the G/P/S model. *Handbook of research on improving learning and motivation through educational games: Multidisciplinary approaches*, *2*, pp.118-136.

Galea, E.R., Owen, M. and Lawrence, P., 1996. The EXODUS model. *Fire Engineers Journal*, pp.26-30.

Knight, J.F., Carley, S., Tregunna, B., Jarvis, S., Smithies, R., de Freitas, S., Dunwell, I. and Mackway-Jones, K., 2010. Serious gaming technology in major incident triage training: a pragmatic controlled trial. *Resuscitation*, *81*(9), pp.1175-1179.

Leyden, J., 2017. *Russian cybercrooks turn on Georgia*. [online] Theregister.co.uk. Available at: http://www.theregister.co.uk/2008/08/11/georgia_ddos_attack_reloaded [Accessed: 19-May-2016].

McMahan, R.P., Bowman, D.A., Zielinski, D.J. and Brady, R.B., 2012. Evaluating display fidelity and interaction fidelity in a virtual reality game. *IEEE transactions on visualization and computer graphics*, *18*(4), pp.626-633.

Miller, B. and Rowe, D., 2012, October. A survey SCADA of and critical infrastructure incidents. In *Proceedings of the 1st Annual conference on Research in information technology* (pp. 51-56). ACM.

Pausch, R., Proffitt, D. and Williams, G., 1997, August. Quantifying immersion in virtual reality. In *Proceedings of the 24th annual conference on Computer graphics and interactive techniques* (pp. 13-18). ACM Press

Smith, R., 2010. The long history of gaming in military training. *Simulation & Gaming*, *41*(1), pp.6-19.

Unity Technologies, "Unity®Pro." 2016.

Wiederhold, B.K. and Wiederhold, M.D., 2008. Virtual reality for posttraumatic stress disorder and stress inoculation training. *Journal of CyberTherapy & Rehabilitation*, *1*(1), pp.23-35.

Veerasamy, N., Grobler, M. and Von Solms, B., 2012, July. Building an ontology for cyberterrorism. In *European Conference on Cyber Warfare and Security* (p. 286). Academic Conferences International Limited.

PREVIOUS ISSUES

2013

Small state performance in the EU decision making process: Case of the IT agency establishment to Estonia. *Ketlin Jaani-Vihalem, Ramon Loik*

The relationships of the willingness for the defence of Estonia among upper secondary school students with the subject 'national defence' taught at school. *Mari-Liis Mänd, Shvea Järvet*

Changes in framing drug issues by the Estonian print press in the last two decades. *Marianne Paimre*

Will efficient punishment please step forth! *Indrek Saar*

Confidence and trust in criminal justice institutions: Lithuanian case *Aleksandras Dobryninas, Anna Drakšienė, Vladas Gaidys, Eglė Vileikienė, Laima Žilinskienė*

Issues of the victimisation experience and fear of crime in Lithuania in the context of restorative justice. *Ilona Michailovič*

2014

Volunteer involvement to ensure better maritime rescue capabilities: A comparative approach to describing volunteering and its motivators by state officials and volunteers. *Jako Vernik, Shvea Järvet*

Crime reducing effects of local government spending in Estonia *Indrek Saar* et al.

Two perspectives of police functions: discourse analysis with the example of Estonia's security policy. *Priit Suve*

Insights into the public defence speciality lecturer's roles in the institution of professional higher education and the controversial role expectations in developing their professional identity. *Anne Valk* et al.

Teaching law enforcement English vocabulary using alternative sources
Ileana Chersan

2015

Fire resistance of timber frame assemblies insulated by mineral wool
Alar Just

Identification parades in Estonia: The state of the art. *Kristjan Kask, Regiina Lebedeva*

The effectiveness of media campaigns in changing individuals' fire, water and traffic safety behavior. *Margo Klaos, Annika Talmar-Pere*

Right-wing extremism and its possible impact to the internal security of the Republic of Estonia. *Ero Liivik*

Crises preparedness of the health care system: Case study analysis in the Estonian context. *Kristi Nero, Shvea Järvet, Jaan Tross*

A framework for training internal security officers to manage joint response events in a virtual learning environment
Sten-Fred Põder, Raul Savimaa, Marek Link

2016

Quantifying the cost of fires in Estonia. *Indrek Saar, Toomas Kääparin*

Some aspects of the design and implementation of an English as a medium of instruction (EMI) course in teacher training:
An example of the Estonian Academy of Security Sciences
Evelyn Soidla, Aida Hatšaturjan, Triin Kibar, Tiina Meos

Immigration of international students from third countries from the perspective of internal security: A case study outcome in comparison of representatives of higher education institutions and officials
Andres Ratassepp, Shvea Järvet, Liis Valk

EDITORIAL POLICY AND DISCLAIMER

The Proceedings of the Estonian Academy of Security Sciences is a non-profit academic journal that publishes well-documented and analysed studies on a full range of contemporary security issues, especially internal security and law enforcement.

Priority is given to the more recent dimensions of international security and risk management developments and innovations, including original case studies, the rise of global security challenges and future perspectives.

The Proceedings considers manuscripts on the following conditions:

- The submitted manuscript is an original work in the field and does not duplicate any other previously published work.
- The manuscript has been submitted only to the Proceedings and is not under consideration for peer-review or has not been accepted for any other publication at the same time, and has not already been published elsewhere.
- The manuscript contains nothing that is morally binding, discriminating or illegal.

By submitting your manuscript you are also agreeing to the necessary originality checks your work may have to undergo during the peer-review, editorial and publishing processes.

All reasonable claims to co-authorship must be clearly named in the manuscript. The corresponding author must be authorised by all co-authors to act on their behalf in all matters pertaining to the publication process. The order of names should also be agreed upon in advance of submission by all authors. The Author must follow the **Harvard style of referencing** and supply all details required by any funding and grant-awarding bodies if appropriate. Authors must also incorporate a statement which will acknowledge any financial interest or benefit they have arising from the direct applications of their submitted study. For all manuscripts a non-discriminatory approach in language usage is mandatory. When using wording which has been or is asserted to be a proprietary term or trademark, the Author must use the symbol ® or TM. There is no submission fee for Proceedings. Fees for Author(s) are exceptional and an object for separate negotiations and agreements. If you wish to include any material in which you do not hold copyright, you must obtain written permission from the copyright owner prior to manuscript submission.

GENERAL REQUIREMENTS FOR THE MANUSCRIPTS

Manuscripts for publication should be submitted in academic English. The Editorial Team accepts Estonian language articles of exceptionally high quality and provides translation to English.

A manuscript should not exceed the limit of 45 000 characters (with spaces). The material in the manuscript should be presented in the following order:

- The full title of the manuscript;
- The name and surname of the author(s), the scientific degree and title, the name of the institution, position, address, phone and e-mail;
- Abstract (500-600 characters);
- The key words (3-5 words);
- The text of the manuscript;
- The list of references (in alphabetical order).

The manuscript should be submitted with single line spacing, normal margins, font type Times New Roman size 12. Justified text alignment is used and paragraphs are separated by a free line or extra spacing.

All headings, except introduction and conclusion, are numbered with Arabic numbers by subdivisions (1., 1.1., 1.1.1). There is no need to start each chapter from a new page or insert superfluous free lines, this will be done by the editor. All tables, figures and pictures used in the article are presented in a separate file with a high resolution (preferably in .jpg, .gif or .pdf format). The scanned images should not be less than 600 dpi, and pictures downloaded from the web should not be less than 100KB in size. A reference is provided in the text as to where the table is supposed to be located.

The Editor reserves the right to abridge and edit submitted texts, as well as to change their titles.

Articles can be submitted throughout the year. However the term of submission of the articles to be published during a given year is the **31st of May.**
The manuscript shall be submitted electronically in .rtf or word format to teadusinfo@sisekaitse.ee.

The publisher reserves the rights to reject or return the manuscripts that do not satisfy the above requirements.

PEER-REVIEW PROCESS

The Proceedings operates on an academic quality policy of double-blind international peer-review. This means that the identity of authors and reviewers are closed during the process.

Submitted manuscripts will be sent to the Editorial Board and then to two or more peer-reviewers, unless the manuscripts are considered to either be lacking in presentation or the written English is below an academic level.

Submitted manuscripts which are not deemed to be out of scope or below the threshold for the journal will be reviewed by two academic experts. Statistical or other relevant topically specialised reviewers are also used where needed. Reviewers are asked to express their competing interests and have to agree to peer-review. Reviewers are asked whether the manuscript is academically competent and coherent, how relevant and important it is and whether the academic quality of the writing is acceptable, as well as suggestions for further revision and improvement of a submitted manuscript.

The final decision is made on the basis that the peer-reviewers are in accordance with one another, or that at least there are no bold dissenting positions. At least one peer-review should be positive in total for the final positive decision. In cases where there is strong disagreement either among peer-reviewers or between the author and peer-reviewers, additional advice is sought from members of the Editorial Board. Additional editorial or external peer-review is also requested when needed. The Proceedings normally allows two revisions of any submitted and peer-reviewed manuscript.

All appeals and claims should be directed to the Editors. The ultimate responsibility for editorial decisions and academic quality lies with the Editorial Board and the Editor-in-Chief.

Reasoned misunderstandings and claims are subject to additional assessment by the Editorial Board in accordance with academic traditions or relevant law.

THIS SPECIAL EDITION OF PROCEEDINGS IS DEDICATED TO

SRIEE
2017
SECURITY RESEARCH,
INNOVATION & EDUCATION EVENT

ORGANISED IN COLLABORATION WITH

SISEKAITSEAKADEEMIA
ESTONIAN ACADEMY OF SECURITY SCIENCES

European
Commission

REPUBLIC OF ESTONIA
MINISTRY OF THE INTERIOR

ISSN 1736-8901 (print)
ISSN 2236-6006 (online)

ISBN 978-9985-67-287-7 (print)
ISBN 978-9985-67-288-4 (pdf)

ISBN 978-9985-67-287-7
9 789985 672877