PROCEEDINGS

Estonian Academy of Security Sciences

■ NUMBER 18 ■ 2019 ■

SECURITY: FROM CORNER TO CORNER

PROCEEDINGS

Estonian Academy of Security Sciences

XVIII

SECURITY: FROM CORNER TO CORNER

SISEKAITSEAKADEEMIA
ESTONIAN ACADEMY OF SECURITY SCIENCES

Tallinn 2019

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 978-9985-67-303-4 (print)
ISBN 978-9985-67-304-1 (pdf)

www.sisekaitse.ee

CONTENTS

FOREWORD

Helina Maasing
Editor-in-Chief

It is my pleasure to introduce the seventh issue of the Proceedings of the Estonian Academy of Security Sciences, which is indexed by the 1.2 Classification of the EBSCO database. Although from an historical point of view, the Estonian Academy of Security Sciences has published original security-related research papers for almost two decades and has hosted the works of more than one hundred authors. The mission of our journal is to foster an academic discussion on scholarly works and research pertaining to internal security.

The current issue of the journal is called from corner to corner. Internal security is not just about fighting crime, protecting borders or being prepared to act to prevent a visible crisis. Effective internal security is much broader, it also means safety in society. The Estonian Internal Security Strategy for 2015-2020 defines security as follows: ensuring security means a stable living environment that ensures both the actual safety of the individual and the individual's feeling of being protected.

When it comes to security and safety, often similar terms are used to define the meaning of these words, but their content allows people to find meaning for themselves. So, if you ask ten different people on the street what security means, it is quite likely that you would get 10 different answers, most of them describing the person's own sense of security.

For some, security means low crime rates; for another, the confidence that a child can walk alone to school in the mornings. Thus, it can be said that security is cognitive and its nature also changes according to the environment.

Similar to the understanding and feeling of people about security, the articles in this journal vary from one corner to another. In this issue security and safety questions are tackled from the corner of cybersecurity to strategic communication to understanding the fire-related risk behaviour of children to security cooperation between states and organisations.

Rain Alev, a recent graduate of Master Studies at the Estonian Academy of Security Sciences, examines in his article counter-terrorism cooperation in the case of the Passenger Name Record between the European Union and the United States. His article points out the obstacles and enablers of the EU-US counter-terrorism cooperation and offers suggestions to make the cooperation more efficient.

Kerli Onno, also an alumni of the Academy, examines in her article how the Baltic States were presented in the Western online media in the context of the Zapad-2017 exercise and indicates lessons for strategic communication.

Piret Pernik researches in her article how to build cybersecurity competences for internal security personnel. The article gives an overview of cybersecurity formal education and extra-curricular initiatives in Estonia, including those supported by the Ministry of Defence. It also gives a snapshot of the state-of-the-art cybersecurity education taking place in the police academies of Finland, Germany, the Netherlands, and Norway, as well as of other international competence building frameworks. The author recommends several policy solutions in order to improve digital skills, cybersecurity and cybercrime competences of future internal security personnel.

Kristjan Kikerpill takes a closer look at the people behind the 'cybercrime' moniker in Estonia. He analyses Estonian court decisions delivered between 01.01.2014 and 10.08.2019. The results show relative uniformity in crimes involving multiple perpetrators, where the primary

distinguishing factor was the level of technical sophistication of the crimes. Crimes committed by individual perpetrators exhibited more variation, ranging from low-tech account takeovers perpetrated by broken-hearted ex-partners to active use of malware and signal jamming devices.

Margo Klaos, Diva Eensoo, Kadi Luht-Kallas and Jaanika Piksööt publish the results of their research about the main personal and environmental variables, which shape children's fire-related risk behaviour. The study was carried out in Estonia with a sample of 903 students from sixth grade classes. The authors analysed the children's safety knowledge, experiences, social environment, and safety education at school compared to their declared frequency of fire-play.

Sille Allikmets is trying to bring more understanding to the concept of good administration in her article "*The place and contents of good administration in Estonian law in the example of terminological diversity based on case-law and the practice of the Chancellor of Justice*".

Ülle Vanaisak is examining the unclear situation of the environmental inspectors (EI) to apply direct coercion. Analysis shows that the number of means of direct coercion the EI inspectors can currently use is not enough to fulfil the tasks stated by the legislator. There is no regulation for the officials' right to self-defence and their direct coercion related training programme needs amending.

Priit Suve in his article uses the study of safety in Estonia as an example to test a framework that helps clarify discovered problems and enhance the quality of information needed for decision making in policing in the context of complexity and uncertainty.

As you see from the short preview of the papers, insecurity may arise from different "corners". The Estonian Academy of Security Sciences is continuing to monitor and research internal security issues from a variety of aspects to provide professionals and societies with additional insights into this interesting world.

THE OBSTACLES AND ENABLERS OF US-EU COUNTER-TERRORISM COOPERATION: THE CASE OF THE PASSENGER NAME RECORD

Rain Alev, MA
Independent researcher

Keywords: United States, European Union, counter-terrorism, terrorism, co-operation, negotiations, international relations, security cooperation, security, complex interdependence, international regime theory.

ABSTRACT

In this article the author examines the European Union (EU) and the United States (US) counter-terrorism cooperation in the case of the Passenger Name Record. The aim of this article is to find the obstacles and enablers of EU-US counter-terrorism cooperation and offer suggestions to make the cooperation more efficient. In addition, the author determines the distribution of resources in this security relationship to make more accurate suggestions. Previous studies suggest that the primary obstacle to counter-terrorism cooperation in the PNR case is *uncertainty* caused by different data protection standards on either side of the Atlantic Ocean. The author used the process tracing method and conducted interviews to determine the obstacles and enablers of trans-Atlantic security cooperation. Although uncertainty was identified as the primary obstacle, it was not caused purely by data protection standards, but also by the fact that the EU was not entirely sure how PNR data would be used after it has been forwarded to Customs and Border Protection by the air carrier. The primary enabler of counter-terrorism cooperation in the PNR case was the more accommodating approach of the US - which led to an agreement. Nevertheless, experts and security strategies suggested that EU-US counter-terrorism cooperation works well and there have been no major problems regarding PNR data exchange.

INTRODUCTION

US-EU counter-terrorism cooperation began to deepen after the 9/11 terrorist attacks, and the years following these attacks saw many new agreements to foster this cooperation. Before 9/11 the EU had not done much to improve trans-Atlantic counter-terrorism cooperation and studies on transatlantic security cooperation were mostly focused on NATO (Gardner & Stefanova, 2001; Spence, 2008; Wolff, 2009; Fahey, 2013, p. 1). After 9/11 however, in 2002 the Council's frame decision pushed member states to set their legislation regarding terrorist crimes and definition of terrorism compatible across member states (Buşe, 2014, p. 48; Council of the European Union, 2002). In 2003 the European Security Strategy (ESS) was adopted, which renewed the EU as a global security actor, by defining the strategic aims and terrorism as the main source of threat (EEAS, 2003; Buşe, 2014, p. 48). Additionally, in 2004 the Hague programme was published as a response to the 9/11 attacks, which set the EU's priorities in the field of internal security (Council of the European Union, 2005a). These documents were followed by a series of agreements between the US and the EU. This article is focused on one of those agreements, the Passenger Name Record (PNR) agreement, which regulates the transfer of air travelers' data between the US and the EU.

After the 9/11 terrorist attacks, the US adopted a legislation which requires air carriers to transfer PNR data to the Department of Homeland Security (DHS) if the flight goes to or through US air space (Fahey, 2013, p. 5). Such a requirement did not comply with the EU's data protection directive, which stipulated an „adequate level of protection" to transferred data (European Parliament and of the Council, 1995). This led to a situation where European air carriers couldn't transfer passengers' data to the DHS due to European data protection regulation and on the other hand, they were supposed to transfer passengers' data if they were flying to the US (Hailbronner *et. al.*, 2008, p. 189). Therefore, US-EU PNR agreements were necessary to regulate the transfer of passengers' data.

The aim of this article is to determine the main obstacles and enablers of the US-EU counter-terrorism cooperation. This article is based on the author's master's thesis and it seeks to summarise and improve the

research done in the thesis. The fact that PNR agreements were concluded three times (four times with the interim agreement) (EU-USA, 2004; EU-USA, 2006; EU-USA, 2007; EU-USA, 2012) could be considered as an indication of the obstacles. In addition, the European Court of Justice (ECJ), having assessed the EU-Canada PNR agreement after such a request by the European Parliament (EP), concluded that the problems that became evident apply to the US-EU agreements as well. These problems included invasion of privacy, inadequate data protection and unclear conditions of data transfer (European Court of Justice, 2017). Earlier studies on this matter have brought out different data protection mechanisms (Hailbronner *et al*, 2008, p. 188) and data protection in general (Archick, 2013, p. 170; Nino, 2010, p. 71; Guild, 2007, p. 2; Byrne, 2012, pp. 7-9) as the main obstacles to the counter-terrorism cooperation. Initative to cooperate and reach an agreement on one or both sides (Yano, 2010, p. 504) and contacts and dialogues between US and EU officials (Archick, 2013, p. 196) have been brought out as enablers of transatlantic security cooperation. In addition, it has been considered an enabler of cooperation when the US prefers negotiating with the EU instead of member states bilaterally (Archick, 2013, p. 196). An enabler of cooperation is therefore a condition which mitigates the obstacles to the cooperation and/or guides towards a better cooperation.

Data protection has been brought out by numerous studies as the central obstacle to transatlantic counter-terrorism cooperation (Nino, 2010, p. 85; Fahey, 2013, pp. 2-4, Hailbronner *et al.*, 2008, pp. 194; Yano, 2010, p. 502; Byrne, 2012, p. 7; Casagran, 2015). The PNR negotiations should reflect these obstacles since PNR as a counter-terrorism instrument involves transferring air travelers' personal data and the different data protection standards of the US and EU. That is why PNR agreements and negotiations are the focus of this article. The theoretical framework used in this study refers to *uncertainty* as the preeminent obstacle to international cooperation (Hasenclever *et al*., 1997, p. 33; Keohane, 1984, p. 97). **This uncertainty is reduced by more efficient cooperation and by the emergence of regimes** (Keohane, 1984, p. 97; Hasenclever *et al*., 1997, p. 36). Therefore, the formulated hypothesis is that the main obstacle to US-EU counter-terrorism cooperation is the uncertainty derived from the differences in data protection.

The importance of studying trans-Atlantic counter-terrorism cooperation is illustrated by the fact that when in 2011 terrorism was considered a very serious security threat by 58% of the EU's population, by the year 2017 that number had increased to 76% (Eurobarometer, 2017, p. 4). Just 4% of the EU's population did not regard terrorism as a threat to the EU's internal security (Eurobarometer, 2017, p. 4). Both in the US and in most of the EU member states, ISIS was considered the primary security threat, especially in the states which had experienced more recent terrorist attacks (Poushter & Manevich, 2017). EUROPOL estimates that around 5000 people from the EU had travelled to conflict regions to join ISIS (EUROPOL, 2017, p. 12). Foreign fighters returning from conflict regions pose a great potential security threat because of their radical views and combat training.

Countering this threat requires law enforcement agencies to cooperate efficiently with other states' agencies and to own an oversight on travellers. Therefore, studying this kind of counter-terrorism cooperation would prove useful in fostering and building cooperation instruments such as PNR. Furthermore, terrorism is increasingly linked to other criminal activities such as the arms trade, drug trafficking and trafficking of persons - as they have become a source of income for terrorist organisations (European Parliament and the Council, 2017). In addition, the EU's PNR directive was adopted in 2016 and it has not yet been fully implemented in the member states. This article could prove useful to officials working in the field of international cooperation regarding security and data transfers as it helps to understand the US-EU security cooperation and data protection's place in this cooperation. Furthermore, this article could be of use to scholars and officials dealing with international cooperation and negotiations, as the author traces negotiation processes and combines it with other research methods to draw conclusions. However, the article could be of most use when dealing with similar security instruments, as the arguments of the sides and methods of influencing the other side are similar.

1. NEGOTIATION PROCESSES

The first PNR negotiations began in December 2003 and were concluded in 2004 (Fahey, 2013, p. 5; EU-USA, 2004). The EU's aim during the negotiations was to include as much data protection as possible, while the US' aim was to guarantee minimal barriers to data transfers (Anagnostakis, 2017, p. 122). The EU got concessions from the US by referring to judicial chaos which would take place in case the PNR agreement was not signed (*threat*) (Anagnostakis, 2017, p. 127). Those concessions were partly possible due to a lack of consensus in the US because the DHS had been pulled into a scandal for illegally collecting PNR data on domestic flights (Baker, 2010, p. 99). However, the European Commission (EC) had been criticised for making demands too soft because the EC was afraid that a too hard stance towards the US would decrease the latter's trust towards the EU and therefore lead to a worse agreement (Interview EU, 2012c ref Anagnostakis, 2017, p. 128). Thus, the lack of consensus in the US and the EU's threats brought the first PNR agreement closer to the EU's aims than the following agreements (Interview US, 2012c ref Anagnostakis, 2017, p. 129). Nevertheless, the first PNR agreement caused a lot of discussion and disapproval in the EU mainly for being unnecessary, disproportional and was labeled as an invasion of the right to privacy as well (Byrne, 2012, p. 7).

The European Parliament (EP) turned to the ECJ, which annulled the EC and the Council of the EU's decisions allowing the signing of the agreement for being judicially based on an incorrect basis (Joined cases C-317/04 ja C-318/04). The ECJ decided that the PNR agreement belongs to the law enforcement area and should therefore be signed in the EU's third pillar framework (Police and Judicial Co-operation in Criminal Matters) not the first pillar framework (European Communities) (Joined cases C-317/04 ja C-318/04). However, the ECJ stated that the first PNR agreement shall stay in force for four months (until September 30) to give time for new negotiations (Joined cases C-317/04 ja C-318/04). This suited the US well because they had wanted to include more of a law enforcement perspective from the beginning of negotiations, since transferring PNR data is not just a data protection issue, but mainly a counter-terrorism and security issue (Anagnostakis, 2017, p. 131). At the same time

however, the EU started to realise the usefulness of PNR data transfers as a counter-terrorism tool (European Report, 2003b ref Anagnostakis, 2017, p. 126) and the preparations to launch the EU's PNR system began in 2007 with a proposal by the EC (Makaveckaite, 2016, p. 9).

The second PNR agreement was signed in 2007 and it was considered less in favour of the EU's demands than the first one as the US used the new negotiations to extend data protection time (De Witte, 2008, p. 11). In the first agreement, PNR data could be shared between agencies only under strict rules and the DHS found it greatly restrictied the US' counter-terrorism capabilities (Baker, 2006; Baker, 2010, pp. 100-101). The US' position in the second negotiations was strengthened by the fact that the alternative to a US-EU agreement was the US signing a number of bilateral agreements with the EU member states (t*hreat*) (Byrne, 2012, p. 6). Therefore, the annulation of the agreement by the ECJ was beneficial to the US and decreased the EU's power in the negotiations (Anagnostakis, 2017, p. 131). Thus, the EU's aim in the negotiations was to preserve the agreement's *status quo* and only change the judicial basis (UK House of Lords, 2007, p. 43). The EC officials emphasized that the second agreement's content should remain the same and only the judicial basis should be changed, because the ECJ did not comment on the content of the agreement (Schofield & Tardy, 2006; Associated Press International, 2006a). The US on the other hand, wanted to immediately sign an agreement with changes to the content and make the sharing of PNR data between agencies more flexible and add more PNR data fields to be collected (Baker, 2010, p. 122; US Fed News, 2006; Associated Press International, 2006b).

In the negotiations the EU used two tactics. Firstly, the EU threatened with the consequences (judicial chaos) if the US should withdraw from the negotiations (*threat*). Furthermore, the EU's negotiators said that the air carriers might decline from sharing PNR data or even not fly to the US at all (*threat*) (International Herald Tribune, 2006a; Baker, 2010, p. 125). Secondly, the EC negotiators said that if the first agreement should expire, the US data protection standards would not be deemed adequate by the EU and it would stop Canada from sharing PNR data with the US (*politicisation*) (Baker, 2010, pp. 125-126). The US turned bilaterally to the EU member states to ascertain their governments' positions should the agreement expire (US Cable, 2006a; US Cable, 2006b; US Cable,

2006e). The US found out that France (US Cable, 2006c), Germany (US Cable, 2006d), Italy (US Cable, 2006e) and Czech Republic (US Cable, 2006b) would be willing to transfer PNR data even if the US-EU negotiations would stop. The US was ready to negotiate with member states bilaterally in case an agreement with the EU was not reached (*threat*) (Agence France-Presse, 2006b). Furthermore, British Airways and Air France were ready to transfer PNR data to the US even if that would have caused court cases in the EU (The Independent, 2006; US Cable, 2006c). Therefore, the fragmentation inside the EU and the positions of the air carriers both weakened the EU's position in the negotiations.

The EU's negotiators did not have the mandate to meet the US' demands and the negotiations stopped on September 29 (Agence France-Presse, 2006a). The absence of an agreement did not cause a judicial chaos nor cancellation of trans-Atlantic flights, and air carriers continued transferring PNR data to the US authorities (European Report, 2006b ref Anagnostakis, 2017, p. 134). Thus, the EU needed an agreement more than the US and an interim agreement was signed on October 6 (Agence France-Presse, 2006b). Signing an interim agreement was also suggested by the EP so that it could take into consideration the shortcomings pointed out by the PNR agreement joint review team (European Commission, 2004b) and the suggestions by the European Data Protection Supervisor (EDPS) (European Parliament, 2006). In the interim agreement however, the US made concessions so that the agreement would be suitable to both sides (*side payment*) as the DHS agreed to share data with other agencies only under certain conditions and the data retention period remained the same (Baker, 2010, p. 138).

As the negotiations restarted in 2007, the EU made new concessions regarding data sharing and the data retention period (Associated Press International, 2007). The EU was in a weak position because its main influencing method (threat of judicial chaos) did not work and the EU could not let the US sign the agreement with member states bilaterally, because then it would not have been able to include it's data protection standards in the agreement (Anagnostakis, 2017, p. 134; (Agence France-Presse 2006b). During the negotiations, the US' negotiators made it clear on several occasions that some topics are a matter of national security and there will be no concessions made (*agenda control*) and threatened to withdraw from the negotiations (*threat*) (Interview EU, 2012c ref

Anagnostakis, 2017, p. 135). The US' aim was to sign a new, more flexible agreement which was not so detailed and based more on trust and principles (Anagnostakis, 2017, p. 135). In addition, the US started promoting the idea that data protection in the US and data protection in the EU offer the same level of protection regardless of differences (*persuasion*) (Federal News Service, 2007a; Federal News Service, 2007b).

In the second PNR agreement, the data retention period was extended to 15 years (EU-USA, 2007). Furthermore, PNR data could be shared with any US agency with even a slight counter-terrorism function and the list of agencies allowed to process PNR data was extended (Baker, 2006; Hailbronner *et. al.*, 2008, p. 191). Since the US promoted the idea of an equal level of data protection, a text emphasizing the similar approach to data protection was added to the preamble of the agreement (EU-USA, 2007). This showed that the EU was unable to force its data protection standards on the US.

The Lisbon Treaty which entered into force on 1 December 2009 increased the power of the EP and any new agreements would have needed the EP's approval (Anagnostakis, 2017, p. 137). 2007). By the time the Lisbon Treaty entered into force, the 2007 PNR agreement had not been ratified in all the EU member states and therefore the EP demanded that a new agreement is signed with better consideration of the EP's demands (Anagnostakis, 2017, p. 137). The EP's opinion was that a new agreement must be in accordance with the EU's data protection standards and using API (Advanced Passenger Information) data as an alternative to PNR should be considered because it's less intrusive regarding a person's privacy (European Parliament, 2011). Furthermore, the EP demanded that the processing of data would only be allowed on a certain case basis and that PNR data will not be used for data mining, otherwise the EP would not give its approval (*threat*) (European Parliament, 2011).

The third agreement was reached in 2011 and the EP gave its approval in April 2012 (Anagnostakis, 2017, p. 115). The US was not interested in a new agreement, but eventually agreed to negotiate on the condition that the new agreement would not decrease the PNR agreement's operational effectiveness and additions regarding security would be made (States News Service, 2011a ref Anagnostakis, 2017, p. 136). As in the previous negotiations, the US threatened withdrawing from the negotiations

(*threat*), which decreased the EU's power (Interview EU, 2012a ref Anagnostakis, 2017, p. 137). In addition, the US linked PNR data sharing to the visa waiver program to ensure support from the EU member states (*promise*) (Anagnostakis, 2017, p. 137). However, the US made concessions because the new agreement had to be acceptable to the EP (*side payment*) (Interview US, 2012d; Interview EU, 2012c ref Anagnostakis, 2017, p. 137). In February 2010, the EP had rejected the US-EU financial data sharing agreement, and this was shocking to the US (Europolitics, 2010b ref Anagnostakis, 2017, p. 136). That kind of power demonstration by the EP showed to the US that the EP is willing to reject the agreement, and this strengthened the EU's position in the negotiations. As during the previous negotiations, the EP demanded that the new agreement was in accordance with the EU's data protection standards and that data mining was excluded (European Parliament, 2012).

The US started lobbying the members of the EP and member states (*persuasion*), which was simplified by the fact that in the EP elections in 2009, right wing conservatives who are traditionally US-friendly gained more seats in the EP (Agence France-Presse, 2010; Europolitics, 2010a ref Anagnostakis, 2017, p. 136; Federal News Service, 2011a). Furthermore, the US offered the visa waiver program to the member states who were willing to cooperate (*side payment*) (European Report, 2007b ref Anagnostakis, 2017, p. 136). This worried some members of the EP that if they vote against the PNR agreement, it would harm their home country's chances to get the visa waiver program (Europolitics, 2010b ref Anagnostakis, 2017, p. 136; Europolitics, 2011 ref Anagnostakis, 2017, p. 136). Likewise, the US warned that if the EP should reject the PNR agreement, there will not be new negotiations (*threat*) (Pop, 2010). This would have meant that none of the EU's data protection standards would apply to the PNR data transferred to the US and therefore, the US' withdrawal from the negotiations would have harmed the EU more than the US (Anagnostakis, 2017, p. 138). Furthermore, the US promoted the idea of an equal level of data protection (*persuasion*) (Federal News Service, 2010; Federal News Service, 2011b).

Although the third PNR agreement has been criticised for unclear or inadequate data protection regulation, the EDPS considers it more in accordance with the EU's data protection standards (Fahey, 2013, p. 7; European Data Protection Supervisor, 2012). In general, the agreement

favors the US, offers a lot of room for interpretation in different legal systems (the Anglo-American and the Continental European) and freedom of action for the DHS (European Data Protection Supervisor, 2012; Fahey, 2013, p. 8). EDPS considered the conditions for using PNR data relatively vague, the data fields being collected to be too many, the data retention period to be too long and stated that the review team should be more independent and capable (European Data Protection Supervisor, 2012).

The joint review team consists of representatives of the EC and DHS, as well as data protection and law enforcement experts (European Commission, 2013). The first PNR agreement review team concluded that despite the criticism of the EU, the DHS has mostly been operating correctly (European Commission, 2004b). Although, the US did not allow the review team access to some of the logs, and some human rights violations were detected (Fahey, 2013, p. 10). However, the interim agreement review team found that the EU was granted enough information, the DHS had performed its duties and that the PNR agreement as a counter-terrorism instrument had been serving its purpose (Joint review report, 2010). In 2013, the review team stated that the DHS had been operating within the boundaries of the agreement and had even exceeded their obligations towards the EU (European Commission, 2013).

The major problems in the PNR negotiations could be summarised as follows (Byrne, 2012, pp. 7-8):

- Number of data fields being transferred – the more data fields are transferred, the bigger the risk of an innocent person being detained.

- Data retention period – the PNR data retention period is 15 years, and even though the PNR data is made anonymous, it could be linked to a person.

- Access to PNR data – while the earlier PNR agreements included a list of agencies with access to the data, the last PNR agreement does not limit the agencies with a list.

- Sharing PNR data with third countries by the US.

- The conditions for using PNR data are unclear – PNR data could be used for crimes punishable with three years of imprisonment or more, which is quite a broad definition.

- Lack of serious compensation for people who have experienced injustice because of PNR data analysis.

- There is no oversight on PNR data sharing – even though there is a joint review team, there are no enforcement mechanisms.

Strategically, the EU had a weaker position since the negotiations launched because the US threatened European air carriers with fines or not allowing them to land on US soil (Spiteri, 2004). Therefore, a hard stance by the EU could have resulted in a significant economic loss because trans-Atlantic flights and trade would have suffered (Anagnostakis, 2017, p. 123). In 2006 it became clear that the air carriers would rather accept the US' demands than follow the EU's data protection regulations (Interview EU, 2012c ref Anagnostakis, 2017, p. 123). In addition, air carriers stored their PNR data in four different databases (Sabre, Galileo, Worldspan and Amadeus) and only one of these databases (Amadeus) was physically located in the EU (Hasbrouck, 2010). Theoretically, this would have meant that even if the air carriers refused to transfer PNR data to the DHS, the US authorities could have still accessed the data (Schwartz & Maynard, 2004). Finally, as mentioned above, as an alternative to an US-EU agreement, the US could have negotiated with member states bilaterally by offering the visa waiver program in return. Therefore, the EU was in a weaker position since the beginning of the negotiations and the EU needed the agreement more than the US did. In 2016 the EU and the US signed a new treaty regarding protection of transferred data, which is known as the Umbrella agreement. However, this treaty is left out of the current study for it involves other security instruments as well.

2. THEORETICAL AND METHODOLOGICAL FRAMEWORK OF THE STUDY

2.1. NEGOTIATIONS AND COOPERATION THROUGH COMPLEX INTERDEPENDENCE AND INTEREST BASED INTERNATIONAL REGIME THEORY

The theoretical framework of this study is combined of *complex interdependence* and *interest based international regime theory*. Complex interdependence according to Keohane and Nye had three main characteristics. First, interdependent states are connected through several channels, such as, for example, power elites and international organisations or companies (Keohane & Nye, 1989, p. 24). Secondly, the relations between states consist of several issues which are not organised in a specific order, there is an absence of hierarchy among issues, foreign policy is affected by domestic policy decisions and thus, the border between foreign and domestic issues is blurred (Keohane & Nye, 1989, p. 25). Thirdly, interdependent states do not use military force against one another because it is not reasonable when addressing economic issues (Keohane & Nye, 1989, p. 25). It is fair to claim that these characteristics apply to US-EU relations.

International regime theories focus on how international institutions, agreements or other systems emerge through negotiations and cooperation (Young, 2005, pp. 92-95). The consensual definition of regimes comes from Krasner, who defined regimes as a „set of indirect principles, norms, rules and executive procedures in which the actors' expectations are close" (Krasner, 1983, p. 2). In general, regimes are related to a specific area (Hasenclever *et al.*, 1997, p. 59), such as trade for example, or, in this study, counter-terrorism. According to Young, regimes are mostly preceeded by negotiations or in his words „institutional bargaining", which is in essence negotiations over establishing an institution (institution does not have to be a formal organisation) (Young, 1991, pp. 282-285; Young & Osherenko, 1993, pp. 225-227). Therefore, it could be said that the US-EU PNR negotiations are a process of regime formation and counter-terrorism cooperation is a regime, which is, in this study, based on the PNR agreement.

Both theories are focused on international cooperation and have a similar approach to cooperation. These theories offer a variety of tools to help analyse the negotiations. Such tools include different theoretical actions to influence the other party in negotiations. These influence tools are listed among relevant theoretical terms in Table 1. In addition, theories offer several indicators to evaluate cooperation. The theoretical methods of influencing listed in Table 1 and theoretical framework in general is the author's interpretation for this study specifically. The US-EU counter-terrorism cooperation in this study is considered a regime based on the PNR agreement. Although the US-EU security cooperation involves other agreements, such as the Mutual Legal Assistance (MLA) agreement, Europol-US agreement or Terrorist Finance Tracking Programme (TFTP), this study focuses solely on the PNR agreement for better focus.

TABLE 1. Relevant theoretical terms (compiled by author)

Term	Meaning	Example
Agenda setting and control (method of influencing)	Pushing favored issues to or moving them in the agenda (Carroll & McCombs, 2003, p. 36).	The EU tells the US that some topics are not negotiable, hence moving them out of the agenda.
Uncertainty	Main obstacle to international cooperation (Hasenclever et al., 1997, p. 33).	The EU and the US can't reach an agreement regarding transfer of passengers' data because the EU considers the US data protection regulation inadequate.
Side payments (method of influencing)	A concession or giving something to foster cooperation (Hasenclever et al., 1997, p. 52).	The EU offers a reduction in trade tariffs if the US guarantees adequate level of data protection.
Promises (method of influencing)	Promises which help to reach an agreement or foster cooperation (Hasenclever et al., 1997, p. 51).	The US promises to proactively send analysed material extracted from PNR data if an agreement is reached.
Politicisation (method of influencing)	Making an issue a political issue so that it is moved up in the agenda and/or receives more attention (Keohane & Nye, 2001, p. 28).	The US links inter-agency data sharing with national security to make data sharing more important in the agenda.
Issue linkage (method of influencing)	Linking one issue to another to make the agenda more suitable (Keohane & Nye, 2001, p. 32).	The EU links data protection with the EU's basic rights to make adequate data protection more important.

TABLE 1 CONTINUED

Persuasion (method of influencing)	Persuading the other actor that cooperation is beneficial (Hasenclever et al., 1997, p. 51).	The US persuades the EU that cooperation is mutually beneficial because processed data is being sent back to the EU.
Distribution of resources	Distribution of resources on a certain issue which is shown in an agreement (Keohane & Nye, 2001, p. 43).	Distribution of resources favours the EU because the EU achieved all its objectives in the agreement.
Regime	A set of principles, norms and procedures in which actors' expectations are similar (Krasner, 1983, p. 2), may but does not have to be based on an agreement	Western democracies form a regime, different agreements among those states foster the existing or create a new, specific regime.
Threat (method of influencing)	Threats to reduce the willingness of the other actor to withdraw from negotiations (Hasenclever et al., 1997, p. 51).	The EU tells the US that if an agreement is not signed, trans-Atlantic flights will stop and legal chaos will take place.

2.2. METHODOLOGICAL APPROACH

To achieve the aim of the study, the author has raised four research questions: (1) what are the obstacles and enablers of the US-EU counter-terrorism cooperation found in the PNR negotiations; (2) what are the similarities and differences in the security strategies with regard to transatlantic security cooperation; (3) which side dominates the US-EU counter-terrorism cooperation relations; (4) how to improve the efficiency of the US-EU counter-terrorism cooperation. The second question is included to find out whether there are fundamental differences in strategic documents regarding counter-terrorism or security cooperation. Security strategies are examined to find out if there are differences in approaching one another which might become obstacles to cooperation. Finding out which side dominates the counter-terrorism relations gives background information to draw conclusions and offer suggestions.

Research tasks were set as follows: (1) analyse the negotiation processes to determine the distribution of resources, obstacles and enablers to the cooperation; (2) analyse the selected strategies and conduct expert interviews to determine obstacles and enablers to the cooperation; (3) offer suggestions to improve the cooperation. To achieve the aim of this study,

the author conducted semi-structured expert interviews and compared security strategies using the document review method. The negotiation processes were reviewed and evaluated using the process tracing method, starting from 2004 when the first PNR agreement was signed.

The author uses the process tracing method to examine the negotiation processes. The process tracing method is used in case studies to learn about causal mechanisms which have led to a certain outcome and make generalised inferences about similar causal mechanisms (Beach, 2017, p. 1). To examine the processes, one has to unpack the causal process and look for traces of action by the actors involved (Beach, 2017, p. 5), which is done in this study by describing the negotiations. Such traces of actions are found in official documents, studies by other authors, international agreements, legislation or media for example. The parts of mechanisms are defined by the actors involved whose actions evoke changes in the outcomes (Beach, 2017, p. 6). In addition, one has to be aware of contextual conditions which are relevant aspects of the background which affect the outcome (Falleti & Lynch, 2009, p. 1152). This systems approach to process tracing has been used in social sciences by Glennan (1996, 2002), Beach & Pedersen (2013, 2016) and many others. The possible actions of actors are described above as methods of influencing and the author looks in the empiric materials for traces of such actions. Possible actions are presented in the Table 1 as theoretical methods of influencing.

Comparison of the results from process tracing, security strategy analysis and expert interviews show whether the obstacles and enablers are similar or not and therefore validate one another. Determining the distribution of resources shows which side dominates the counter-terrorism relations and therefore helps to understand the cooperation relationship and to find obstacles or enablers. For example, when one state is dominating but makes concessions in the negotiations, that state reduces the obstacles to reaching an agreement and therefore this action works as an enabler to cooperation. Cooperation is when actors adjust their behavior to the preferences of others, through a process of policy coordination (Keohane, 1984, p. 52). Cooperation efficiency is hence shown by how well two actors can adjust their behavior to the preferences of others.

Firstly, the author will compare the security strategies to find fundamental differences regarding trans-Atlantic security cooperation as

obstacles to the cooperation or similarities to determine enablers of the cooperation. Secondly, the author will examine the negotiations presented in the negotiation processes description to find out which methods of influencing were used, how much they were used and how did it change the course of reaching an agreement or what kind of distribution of resources does it indicate. Thirdly, the author will analyse the expert interview transcriptions qualitatively to present the conclusions, main findings and viewpoints of the interviewed experts. Finally, the author will combine the findings to make final conclusions and to achieve the aim of the article.

3. DIFFERENCES AND SIMILARITIES INDICATED BY SECURITY STRATEGIES

Qualitative analysis of the security strategies makes it possible to see whether the US and EU have a different approach on trans-Atlantic security cooperation. A different approach on the strategic level might be an obstacle to cooperation and a similar approach might be an enabler. In this study, the author looks for differences and similarities regarding trans-Atlantic security cooperation in relevant strategies.

From the US strategies, the author selected the National Security Strategies (NSS) of 2002, 2010 and 2017 and Counter-Terrorism Strategy (CTS) from 2006 (United States, 2002; United States, 2006; United States, 2010; United States, 2017). From the EU strategies, the author selected the EU Security Strategy from 2003, CTS from 2005, Internal Security Strategy from 2010 and EU Foreign and Security Policy from 2016 (EEAS, 2003; Council of the European Union, 2005b; Justice and Home Affairs Council, 2010; EEAS, 2016). The author points out that the EU is a constantly changing international organisation and therefore over time the strategies have changed in their form. Whereas the NSS has stayed pretty much the same during those years. The author coded segments which directly concerned trans-Atlantic security cooperation.

TABLE 2. Coded segments in strategies (compiled by author).

Document	Coded segments
USA National Security Strategy 2002	7
EU Security Strategy 2003	3
EU CT Strategy 2005	1
USA CT Strategy 2006	1
EU Internal Security Strategy 2010	0
USA National Security Strategy 2010	4
EU Global Strategy for Foreign and Security Policy 2016	6
USA National Security Strategy 2017	4

In general, the strategies did not show any differences in the approach to trans-Atlantic security cooperation. Cooperation has been considered important and there is a will to strengthen it further on both sides. It seems that the EU aims to become a more equal and global security actor and that the US is more emphasized on trade relations. There are no fundamental differences in the security strategies regarding trans-Atlantic security cooperation and both sides consider each other very important partners in counter-terrorism cooperation. (Alev, 2019, p. 54-56)

3.1. THE METHODS OF INFLUENCING USED BY BOTH SIDES

The primary goals of the actors found in the description of the negotiations could be summarised as follows:

- The US aims: to guarantee free inter-agency data transfers and data processing; not to make any changes in the US legislation; to base the agreement on shared principles and mutual trust.

- The EU aims: to guarantee as much EU data protection as possible on the transferred data.

TABLE 3. The methods of influencing used by the US and the EU during the negotiations (compiled by author).

Method of influencing		US	EU
Issue linkage	Politicisation	1	1
	Promises	1	-
	Threats	5	5
Side payments		2	-
Persuasion		2	-
Agenda setting and control		1	-
Total		10	6

The traces of the processes are found in the description of the negotiation processes. The theoretical methods of influencing allow us to determine

which side is dominant and/or more active. Determining the dominant side helps to understand the cooperation because the dominant side might be determinant on reaching the agreement. When the dominant side makes more concessions than it should, its actions might be an enabler of the cooperation. Table 3 shows that the US used more methods of influencing than the EU and the US used all the theoretical methods at least once. This might indicate that the distribution of resources favoured the US. The EU on the other hand, only used politicisation and threats.

The least influencing methods were used during the 2004 agreement negotiations. That might be due to the urgent need for an agreement and the fact that the EU's threat tactic worked. The most influencing methods were used during the negotiations for the interim and the second agreement. One might presume that this was caused by the EU's strategically weak position in the second negotiations. The EU's position was weak because the alternative for the US-EU agreement would have been bilateral agreements between the US and EU member states, which would have been unacceptable to the EU as a global security actor. On the other hand, it is likely that the US would have still preferred negotiating with the EU since then it would not have been necessary to negotiate separate agreements with each of the member states. (Alev, 2019, p. 57, 61)

The EU's threat tactics didn't work after the first negotiations because member states and air carriers were willing to cooperate with the US regarding PNR data transfers. The US used agenda control and persuasion during the 2007 negotiations, which proved to be successful because some topics were pushed off the agenda and the EU agreed that the approach to data protection was similar. It's safe to say that the 2007 agreement was the most in favor of the US because it has received the most criticism from actors inside the EU and the EU's position was the weakest of the three negotiations. In 2011, the EU's position was strengthened by the EP and it's right to veto the agreement and this led to an agreement which favored the EU more than the previous agreement. The EU's position was weakened by the fragmentation inside the EU. By the 2015 joint review however, it seems that both sides were happy with the agreement and that it works well as a counter-terrorism instrument. In conclusion, it could be said that the US achieved more of its aims than

the EU. The distribution of resources favored the US because it achieved more of it's aims than the EU. (Alev, 2019, p. 57, 61)

Process tracing suggests that an obstacle to the cooperation was primarily the difference in data protection because most of the issues during negotiations were related to data protection. The fact that the EU did not trust its citizens' personal data to be transferred to the US, suggests uncertainty – which was brought out as the main obstacle to cooperation by Keohane. Therefore, a regime was created (PNR agreement was signed) to reduce the uncertainty and increase trust in that matter. Besides, that points to the productive effect of uncertainty. As an enabler of cooperation, side payments by the US could be brought out because they led to an agreement. Furthermore, initiative shown by the US in the form of a more active use of influencing methods, could be considered an enabler to the cooperation. A learning process which occurred in the EU by understanding the possible benefits of the EU's PNR system, could also be considered an enabler of cooperation. (Alev, 2019, p. 57, 61)

3.2. EXPERT ASSESSMENTS ON COUNTER-TERRORISM COOPERATION

The author conducted seven semi-structured expert interviews. The interviewees were two data protection experts, one law enforcement expert and four experts from the negotiations and political field. The interviews concluded that mutual initiative is as an enabler of cooperation. In addition, there is a general and mutual consensus between the US and the EU regarding counter-terrorism. The experts considered the current PNR agreement and system as optimal and reasonable. Reopening the negotiations was not supported by any of the interviewees, but it might become necessary in the future as technology and the security environment are evolving. (Alev, 2019, p. 69)

The EU's data protection standards were considered as the main obstacle to the cooperation because the EU demanded that the US followed the EU's standards as much as possible. Different legal systems were also brought out as an obstacle. Although, most of the interviewees did not name uncertainty as an obstacle, all of them expressed fears or distrust

regarding the data protection issue in PNR negotiations. This supports the hypothesis that the main obstacle to cooperation was uncertainty caused by different data protection standards, since data protection was named as the main obstacle. Some of the interviewed experts brought out the EU's learning process, as over time the EU understood the potential benefits of the PNR system and thus, the learning process could be considered as an enabler of cooperation. The interviews support the theoretical claim that uncertainty may have a productive influence as it pushes two actors to a better cooperation to reduce the uncertainty. The interviewees brought out the EU's fragmentation as an obstacle as it weakened the EU's position in the negotiations. However, all the interviewees considered the fragmentation inevitable. (Alev, 2019, p. 67-70)

4. CONCLUSIONS AND RECOMMENDATIONS

The first research question was provided an answer from process tracing and expert interviews. Process tracing and interviews showed that the main obstacles to cooperation were different data protection standards, because most of the issues in the negotiations were related to data protection. Therefore, it was uncertainty on the EU side because the US' data protection was deemed inadequate. The main enablers of cooperation were concessions and side payments by the US and a mutual initiative to reach an agreement.

The second research question was provided an answer by the comparison of security strategies. There were no fundamental differences regarding trans-Atlantic counter-terrorism cooperation. In general, the EU and the US see each other as core partners combating different security challenges. Therefore, there were no clear discrepancies in security strategies.

The third research question was provided an answer from process tracing and expert interviews. The EU's position was weaker because their threat tactics did not work after the first negotiations and air carriers and member states were willing to cooperate with the US in the absence of an agreement. Inclusion of the EP after the Lisbon Treaty strengthened the EU's position because the US was forced to make the agreement suitable to the EP. The US achieved its aims more than the EU. The EU did not have much to bargain with in the negotiations, which is shown by the use of the influencing methods. Therefore, the distribution of resources favored the US and the US is the dominant actor in the trans-Atlantic counter-terrorism cooperation.

The fourth research question is provided an answer by the results of process tracing and expert interviews. Improvements in this case mean reducing the obstacles and enhancing the enablers of cooperation. Since one of the named obstacles was the fragmentation inside the EU, counter-terrorism cooperation could be improved by better coordination inside the EU, which would enable the EU to set aims that would not be harmed by the EU's fragmentation. Additionally, trans-Atlantic

counter-terrorism cooperation could be improved by changing the EU's data protection legislation to become more compatible with the one in the US, as it would help to reach future agreements faster. However, it is highly unlikely, and it requires initiative from the EP, EC and member states. Cooperation could also be improved by making side payments, which do not have to be in the same field or in the same negotiations. In addition, effective communication inside the EU and educating different interest groups could fasten the learning process and therefore make reaching an agreement easier.

TABEL 4. Obstacles and enablers of cooperation with suggestions (compiled by author).

Obstacle of cooperation	Suggestion
Different data protection standards	Changing data protection regulation to be more compatible
EU's fragmentation	More effective coordination among member states, the EP and EC
Uncertainty	Forming regimes (frameworks and agreements)
Enabler of cooperation	Suggestion
Mutual initiative	Sustaining effective partnership
Side payments	Use more side payments to reach an agreement
Learning process	Educating interest groups, effective communication

This paper's aim was to determine the obstacles and enablers of the US-EU counter-terrorism cooperation by analysing PNR negotiations and offer suggestions to improve the cooperation. The process tracing method showed that the distribution of resources favored the US and data protection became the central issue in the negotiations. The EU's weaker position in the negotiations was illustrated by ineffective use of influencing methods and internal fragmentation. However, the EP entering the negotiations strengthened the EU's position. Uncertainty regarding data transfers became the main obstacle to reaching an agreement.

The US used more influencing methods than the EU and therefore was the more active side and this supports the claim that the US was in a stronger position. The US was the dominant side because it was in

a stronger position in the negotiations. Side payments by the US can be considered as an enabler of the cooperation since it made reaching an agreement easier. The analysis of security strategies did not show a fundamental difference in approach to trans-Atlantic counter-terrorism cooperation, but showed that both actors see each other as core partners in the fight against terrorism. This claim was supported by interviewed experts who stated that there is a fundamental consensus regarding counter-terrorism cooperation. The interviewees also concluded that the EU's data protection became an obstacle in the negotiations. Both the interviews and process tracing support the hypothesis that uncertainty caused by different data protection standards was the main obstacle to the cooperation.

Since uncertainty became the main obstacle to the cooperation and uncertainty is reduced by forming new regimes (agreements, frames), cooperation would be improved by different agreements in specific fields that would make different data protection systems more compatible. The fragmentation inside the EU could be reduced by better coordination among member states, the EP and EC to maximise the common ground. As mentioned above, this article could prove useful to officials and scholars dealing with US-EU security cooperation, international negotiations or cooperation instruments related to data protection. The findings of this article could be used by the EU officials preparing for negotiations in similar fields to security cooperation or dealing with negotiations over a certain instrument with similar characteristics as the PNR negotiations. Since the methods of influencing in international negotiations should be the same as presented in this study, the findings and methodology in this study could be used to analyse cooperation and negotiations by scholars or officials. These findings could also be used by officials from the EU member states to influence the policies and processes to move in a preferred direction.

In further studies, other security cooperation instruments (such as MLA or TFTP) and their processes could be studied using similar methodology. This would help build a bigger picture of the US-EU security or counter-terrorism cooperation and its dynamic. In addition, the presented methods of influencing or the use of such methods could be studied as it helps to better understand and use these methods in negotiations. The findings of this article could be used

in comparison to these potential future studies. Furthermore, the recently adopted General Data Protection Regulation (GDPR) of the EU could be involved in such studies to determine the effect it has on trans-Atlantic security cooperation and data transferring.

Contact:

Rain Alev
E-mail: rain95.alev@gmail.com

REFERENCES AND SOURCES

Agence France-Presse, 2006a. US sends air passenger-data draft agreement to EU. *Agence France-Presse*, October 1.

Agence France-Presse, 2006b. EU, US Clinch air passenger data deal. *Agence France-Presse*, October 6.

Agence France-Presse, 2010. US seeks to persuade EU deputies to back terror data deal. *Agence France-Presse*, March 8.

Alev, R., 2019. *Euroopa Liidu ja Ameerika* Ühendriikide *terrorismivastase koostöö takistused ja võimaldajad lennureisijate broneeringu infosüsteemi (PNR) rakendamise näitel. Master's thesis*. Tallinn: Estonian Academy of Security Sciences. [Online source] Available from: https://digiriiul.sisekaitse.ee/bitstream/handle/123456789/2221/2019_Alev%20.pdf?sequence=1&isAllowed=y [Accessed 25.09.2019].

Anagnostakis, D., 2017. *EU-US Cooperation on Internal Security: Building a Transatlantic Regime*. Oxon: Routledge.

Archick, K., 2013. U.S.-EU Cooperation Against Terrorism. *Current Politics & Economics of Europe*, 24(1/2), 169-201, pp. 169-201.

Associated Press International, 2006a. EU justice, interior ministers study plans to salvage trans-Atlantic passenger data deal with US. *Associated Press International*, June 2.

Associated Press International, 2006b. EU likely to close deal with Washington on new anti-terror passenger data. *Associated Press International*, September 27.

Associated Press International, 2007. EU ambassadors back deal with US on sharing air passenger data. *Associated Press International*, June 29.

Baker, S., 2006. *Letter to the Council Presidency and the Commission from the Department of Homeland Security (DHS) of the United States of America, concerning the interpretation of certain provisions of the undertakings issued by DHS on 11 MAY 2004 in connection with the transfer by air carriers of passenger name record (PNR) data. Letter.* [Online source] Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1549917977001&uri=CELEX:52006XG1027(01) [Accessed 19.02.2019].

Baker, S., 2010. *Skating on Stilts: Why We Aren't Stopping Tomorrow's Terrorism*. Stanford: Hoover Institution Press.

Beach, D., Pedersen, R., 2013. *Process-tracing methods: Foundations and guidelines*. Ann Arbor: University of Michigan Press.

Beach, D., Pedersen, R., 2016. *Causal case studies: Comparing, matching and tracing*. Ann Arbor: University of Michigan Press.

Beach, D., 2017. Process-Tracing Methods in Social Science. *Oxford Research Encyclopedia of Politics*. 25 January.

Buşe, M., 2014. Terrorism – a current threat to European security. *Strategic Impact*, 50(1), pp. 45-54.

Byrne, A., 2012. *Building the Transatlantic Area of Freedom, Security and Justice. The Case of the Passenger Name Record Agreements. Presentation*. Rome, Istituto Affari Internazionali 15 March 2012 seminar: The Challenges in Creating a Transatlantic Area of Freedom, Security and Justice.

Carroll, C. E., McCombs, M., 2003. Agenda-setting Effects of Business News on the Public's Images and Opinions about Major Corporations. *Corporate Reputation Review*. 6(1), pp. 36-46.

Casagran, C., 2015. The Future EU PNR System: Will Passenger Data be Protected?. *European Journal of Crime, Criminal Law & Criminal Justice*. 23(3). pp. 241-257.

Council of the European Union, 2002. *Council Framework Decision of 13 June 2002 on combating terrorism*. [Online source] Available from: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32002F0475 [Accessed 31.08.2019].

Council of the European Union, 2005a. *The Hague Programme: strengthening freedom, security and justice in the European Union. Strategy.* [Online source] Available from: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52005XG0303(01) [Accessed 31.08.2019].

Council of the European Union, 2005b. *The European Union Counter-Terrorism Strategy*. Brussels: Council of the European Union. [Online source] Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=LEGISSUM%3Al33275 [Accessed 31.08.2019].

De Witte, B., 2008. Too much constitutional law in the European Union's Foreign Relations? Book: Cremona, M., De Witte, B., ed. *EU Foreign Relations Law: Constitutional Fundamentals.* Oxford: Hart Publishing.

Eurobarometer, 2017. *Europeans' attitudes towards security. Survey.* [Online source] Available from: https://data.europa.eu/euodp/data/dataset/S1569_87_4_464B_ENG [Accessed 25.09.2019].

European External Action Service (EEAS), 2003. *European Security Strategy - A Secure Europe in a Better World*. Brussels: European Council. [Online source] Available from: https://europa.eu/globalstrategy/en/european-security-strategy-secure-europe-better-world [Accessed 31.08.2019].

European External Action Service (EEAS), 2016. *Shared Vision, Common Action: A Stronger Europe*. Brussels: Council of the European Union. [Online source] Available from: https://europa.eu/globalstrategy/en/shared-vision-common-action-stronger-europe [Accessed 31.08.2019].

European Commission, 2004b. *2004/535/EC: Commission Decision of 14 May 2004 on the adequate protection of personal data contained in the Passenger Name Record of air passengers transferred to the United States' Bureau of Customs and Border Protection*. [Online source] Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32004D0535 Accessed 31.08.2019].

European Commission, 2013. *REPORT FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL on the joint review of the implementation of the Agreement between the European Union and the United States of America on the processing and transfer of passenger name records to the United States Department of Homeland Security.* [Online source] Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1549917977001&uri=CELEX:52013DC0844 [Accessed 31.08.2019].

European Court of Justice, 2017. *The Court declares that the agreement envisaged between the European union and Canada on the transfer of Passenger Name Record data may not be concluded in its current form. Assessment.* [Online source] Available from: http://curia.europa.eu/juris/document/document.jsf?text=&docid=183140&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=13108693 [Accessed 31.08.2019].

European Data Protection Supervisor, 2012. *Opinion of the European Data Protection Supervisor on the proposal for a Council Decision on the conclusion of the Agreement between the United States of America and the European Union on the use and transfer of Passenger Name Records to the United States Department of Homeland Security. Assessment.* [Online source] Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52012XX0209(03) [Accessed 31.08.2019].

European Parliament, 2006. *European Parliament recommendation to the Council on the negotiations for an agreement with the United States of America on the use of passenger name records (PNR) data to prevent and combat terrorism and transnational crime, including organised crime (2006/2193(INI)).* [Online source] Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1549917977001&uri=CELEX:52006IP0354 [Accessed 31.08.2019].

European Parliament, 2011. *European Parliament resolution of 5 May 2010 on the launch of negotiations for Passenger Name Record (PNR) agreements with the United States, Australia and Canada*. [Online source] Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1549917977001&uri=CELEX:52010IP0144 [Accessed 31.08.2019].

European Parliament, 2012. *EU external strategy on Passenger Name Record (PNR) European Parliament resolution of 11 November 2010 on the global approach to transfers of passenger name record (PNR) data to third countries, and on the recommendations from the Commission to the Council*

to authorise the opening of negotiations between the European Union and Australia, Canada and the United States. [Online source] Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1549917977001&uri=CELEX:52010IP0397 [Accessed 31.08.2019].

European Parliament and the Council, 1995. *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data*. *Directive* [Online source] Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A31995L0046 [Accessed 31.08.2019].

European Parliament and the Council, 2017. *Directive (EU) 2017/541 of the European Parliament and of the Council of 15 March 2017 on combating terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA*. [Online source] Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32017L0541 [Accessed 25.09.2019].

EUROPOL, 2017. European Union Terrorism Situation and Trend Report TE–SAT. [Online source] Available from: https://www.europol.europa.eu/activities-services/main-reports/eu-terrorism-situation-and-trend-report [Accessed 25.09.2019].

EU-USA, 2004. *Agreement between the European Community and the United States of America on the processing and transfer of PNR data by air carriers to the United States Department of Homeland Security, Bureau of Customs and Border Protection*. *Treaty.* [Online source] Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1549469893043&uri=CELEX:22004A0520(01) [Accessed 31.08.2019].

EU-USA, 2006. *Agreement between the European Union and the United States of America on the processing and transfer of passenger name record (PNR) data by air carriers to the United States Department of Homeland Security. Treaty.* [Online source] Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1549469893043&uri=CELEX:22006A1027(01) [Accessed 31.08.2019].

EU-USA, 2007. *Agreement between the European Union and the United States of America on the processing and transfer of Passenger Name Record (PNR) data by air carriers to the United States Department of Homeland Security (DHS). Treaty.* [Online source] Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1549917977001&uri=CELEX:22007A0804(01) [Accessed 31.08.2019].

EU-USA, 2012. *Agreement between the United States of America and the European Union on the use and transfer of passenger name records to the United States Department of Homeland Security. Treaty.* [Online

source] Available from: https://eur-lex.europa.eu/legal-content/GA/TXT/?uri=CELEX:22012A0811(01) [Accessed 31.08.2019].

EU-USA, 2016. *Agreement between the United States of America and the European Union on the protection of personal information relating to the prevention, investigation, detection, and prosecution of criminal offences. Treaty.* [Online source] Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:22016A1210(01) [Accessed 31.08.2019].

Fahey, E, 2013. Law and Governance as Checks and Balances in Transatlantic Security: Redress and Remedies in EU-US Passenger Name Records and the Terrorist Finance Tracking Program. *Yearbook of European Law*, 32(1), pp. 368-388.

Falleti, T., Lynch, J., 2009. Context and causal mechanisms in political analysis. *Comparative Political Studies*, 42, pp. 1143-1166.

Federal News Service, 2007a. Remarks by Secretary Michael Chertoff, Department of Homeland Security to the Johns Hopkins Paul N. Nitze School of Advanced International Studies. *Federal News Service*, May 3.

Federal News Service, 2007b. Remarks by Secretary of Homeland Security Michael Chertoff to the European Parliament. *Federal News Service*, May 15.

Federal News Service, 2010. Atlantic Council of the United States (ACUS) Meeting; Subject: "Transatlantic Security, Data Sharing and Privacy Protections: A US-EU Dialogue". *Federal News Service*, July 8.

Federal News Service, 2011a. Hearing of the Europe and Eurasia Subcommittee of the House Foreign Affairs Committee; Subject: Overview of Security in Europe and Eurasia. *Federal News Service*, May 5.

Federal News Service, 2011b. Prepared Remarks of Attorney General Eric Holder to the European Parliament's Committee on Civil Liberties, Justice, And Home Affairs Location: Brussels, Belgium. *Federal News Service*, September 20.

Gardner, H., Stefanova, R., 2001. *The New Transatlantic Agenda: Facing the Challenges of Global Governance*. Aldershot: Ashgate.

Glennan, S., 1996. Mechanisms and the nature of causation. *Erkenntnis*, 44(1), pp. 49-71.

Glennan, S., 2002. Rethinking mechanistic explanation. *Philosophy of Science*, 69, pp. 342-353.

Guild, E., 2007. Inquiry into the EU-US Passenger Name Record Agreement. *CEPS Policy brief*, 125, pp. 1-4.

Hailbronner, K., Papakonstantinou, V., Kau, M., 2008. The Agreement on Passenger-Data and the EU-US Cooperation in Data Communication. *International Migration*, 46(2), pp. 187-197.

Hasbrouck, E., 2010. *Testimony to Members of the European Parliament*. April 8. [Online source] Available from: https://hasbrouck.org/blog/archives/001855.html [Accessed 31.08.2019].

International Herald Tribune, 2006a. EU and US plan deal to share traveller data; Wide-ranging accord expected in weeks. *International Herald Tribune*, September 1.

Joined cases C-317/04 ja C-318/04. (2006) ECLI:EU:C:2006:346.

Joint review report., 2010. *Report on the joint review of the implementation of the Agreement between the EU and US on the processing and transfer of Passenger Name Record data by air carriers to the US Department of Homeland Security, 8-9 February 2010*. [Online source] Available from: https://www.dhs.gov/xlibrary/assets/privacy/privacy_eu_pnr_aircarriers_feb_2010.pdf [Accessed 31.08.2019].

Justice and Home Affairs Council. *Internal Security strategy for the European Union – Towards a European security model*. Brussels: Council of the European Union. [Online source] Available from: https://www.consilium.europa.eu/en/documents-publications/publications/internal-security-strategy-european-union-towards-european-security-model/ [Accessed 31.08.2019].

Keohane, R., 1983. The Demand for International Regimes. Book: S. Krasner, ed. *International Regimes*. Ithaca: Cornell University Press.

Keohane, R., 1984. *After Hegemony: Cooperation and Discord in the World Political Economy*, Princeton University Press.

Keohane, R., Nye, Joseph S., 1989. *Power and Interdependence*. Harvard University: Harper Collins Publishers.

Keohane, R., Nye, Joseph S., 2001. *Power and Interdependence*. New York: Longman.

Krasner, S., 1983. Structural Causes and Regime Consequences: Regimes as Intervening Variables. Book: S. Krasner, ed. *International Regimes*, Ithaca: Cornell University Press.

Makaveckaite, I., 2016. *European Passenger Name Record through the Multiple Streams Framework: The Power of Streams in the Policy Making. Master's thesis*. Leiden: Leiden University.

Nino, M., 2010. The protection of personal data in the fight against terrorism. New perspectives of PNR European Union instruments in the light of the Treaty of Lisbon. *Utrecht Law Review*, 6(1), pp. 62-85.

Pop, V., 2010. Reding slams US over data privacy. *EUobserver*, December 21. [Online source] Available from: https://euobserver.com/news/31555 [Accessed 31.08.2019].

Poushter, J., Manevich, D., 2017. Globally, People Point to ISIS and Climate Change as Leading Security Threats. *Pew Research Center*. [Online source] Available from: http://www.pewglobal.org/2017/08/01/globally-people-point-to-isis-and-climate-change-as-leading-security-threats/ [Accessed 25.09.2019].

Schofield, A., Tardy, M., 2006. Court Scraps European Union-U.S. Passenger Data Agreement. *Aviation Daily*, May 31. [Online source] Available from: http://aviationweek.com/awin/court-scraps-european-union-us-passenger-data-agreement [Accessed 31.08.2019].

Schwartz, J., Maynard, M., 2004. Airlines Gave F.B.I. Millions of Records on Travelers After 9/11. *New York Times*, May 1. [Online source] Available from: https://www.nytimes.com/2004/05/01/us/airlines-gave-fbi-millions-of-records-on-travelers-after-9-11.html [Accessed 31.08.2019].

Spence, D., 2008. Introduction: International Terrorism – the Quest for a Coherent EU Response. Book: D. Spence, ed. *The European Union and Terrorism*. London: John Harper.

Spiteri, S., 2004. EU court asked to rule on EU-US data agreement. *EUobserver*, April 21. [Online source] Available from: https://euobserver.com/justice/15275 [31.08.2019].

The Independent, 2006. Court stops US getting passengers' details. *The Independent*, May 31.

UK House of Lords, 2007. *The EU/US Passenger Name Record (PNR) Agreement. Twenty-First Report*, HL Paper 108(5), June 5.

United States, 2002. *The National Security Strategy of the United States of America*. Washington: President of the U.S. [Online source] Available from: https://history.defense.gov/historical-sources/national-security-strategy/ [Accessed 31.08.2019].

United States, 2006. *National Strategy for Combating Terrorism*. Washington: The White House. [Online source] Available from: https://2001-2009.state.gov/s/ct/rls/wh/71803.htm [Accessed 31.08.2019].

United States, 2010. *The National Security Strategy*. Washington: President of the U.S. [Online source] Available from: https://www.hsdl.org/?abstract&did=24251 [Accessed 31.08.2019].

United States, 2017. *The National Security Strategy of the United States of America*. Washington: President of the U.S. [Online source] Available from: https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf [Accessed 31.08.2019].

US Cable, 2006a. UK Passenger Name Recognition Contingency Planning. *Wikileaks*, July 12. 2006. [Online source] Available from: http://wikileaks.redfoxcenter.org/cable/2006/07/06LONDON5097.html [Accessed 31.08.2019].

US Cable, 2006b. Czech Republic: Positive on PNR Collection. *Wikileaks*, July 14. [Online source] Available from: http://wikileaks.redfoxcenter.org/cable/2006/07/06PRAGUE804.html [Accessed 31.08.2019].

US Cable, 2006c. Air France on PNR, No-Fly and CNIL. *Wikileaks*, September 6. [Online source] Available from: http://wikileaks.redfoxcenter.org/cable/2006/09/06PARIS5958.html [Accessed 31.08.2019].

US Cable, 2006d. DHS Counselor Resenzweig Pushes for CT progress in Berlin. *Wikileaks*, September 12. [Online source] Available from: http://wikileaks.redfoxcenter.org/cable/2006/09/06BERLIN2654.html [Accessed 31.08.2019].

US Cable, 2006e.Passenger Data Sharing Views as Old Agreement Expires. *Wikileaks*, September 27. [Online source] Available from: http://wikileaks.redfoxcenter.org/cable/2006/09/06ROME2724.html [Accessed 31.08.2019].

US Fed News, 2006. Privacy Rights Need to be Respected – Even in Police Cooperation. *US Fed News*, September 27.

Wolff, S., 2009. The Mediterranean Dimension of EU Counterterrorism. *Journal of European Integration*, 31(1), pp. 137-156.

Yano, M. J., 2010. Come Fly the (Unfriendly?) Skies: Negotiating Passenger Name Record Agreements Between the United States and European Union. *I/S: A Journal of Law and Policy for the Information Society*. 5(3), pp. 479-505.

Young, O., 1991. Political Leadership and Regime Formation: On the Development of Institutions in International Society. *International Organization*. 45, pp. 281-308.

Young, O., 2005. Regime theory and the quest for global governance. Book: A. Ba, M. Hoffmann, ed. *Contending Perspectives on Global Governance*. Abingdon: Routledge.

Young, O., Osherenko, G., 1993. International Regime Formation: Findings, Research Priorities, and Applications. Book: O. Young, G. Osherenko, ed. *Polar Politics: Creating International Environmental Regimes*. Ithaca: Cornell University Press.

BALTIC STATES AND THE ZAPAD 2017 EXERCISE IN THE WESTERN MEDIA: IMPLICATIONS FOR SMALL STATE STRATEGIC COMMUNICATION

Kerli Onno, MA
Independent researcher

Keywords: strategic communication, Zapad-2017, Baltic States, media

ABSTRACT

Every now and then, somewhere in the world events take place that are regarded as having International news value. Nowadays, it is easy to become a mediated observer and to have an opinion about something that happens on the other side of the world. In September 2017, the Russian Federation's Zapad military exercise was an event which gained widespread media attention on an international scale. It brought unusually large media coverage to the Baltic States due to their geographic closeness to the exercise area and the fact that the Russian Federation is their most important security threat. The study researches the messages that spread in Western online news media which have a strong potential to influence the perception of the Baltic States among the allies and their societies at large. The aim of this study is to examine how the Baltic States were presented in the Western media in the context of the Zapad-2017 excercise and indicate lessons for strategic communication.

INTRODUCTION

The three small Baltic States share the same main security threats (Veebel, 2018; Vaicekauskaitė, 2018; Bailes, 2013) and the most important of those is the threat from the east, from the Russian Federation. EU and NATO membership has not completely eradicated the security concerns of the Baltic States and the identity of the region has been largely influenced by Russia (Jurkynas, 2007, p. 166). That is the main reason why the Zapad-2017 military exercise brought widespread media attention to the area, and brought along a worldwide discussion about the Russian Federation's threat to the region and to the Baltic States.

Naveh (2005) explains that when it comes to international events, the selection of events and the way they are presented are often influenced by the international political agenda. It is obvious that all states do not get a similar amount of attention and if a small state is presented, it is possible that they play an important part in a great power's interests (Bennet & Paletz, 1994, pp 31; Wanta, Golan & Lee, 2004). Therefore, the media and politics have a two-way relationship: the political agenda influences what is regarded as important and the media has a role in making these events important.

Therefore, the image of a small state is of strategic importance as their security depends largely upon collective defence strategies. To find out what can be learned from the media coverage of the Zapad military excercise in 2017, the research problem of this study was formulated:

How were the Baltic States presented in the Western media in 2017 in the context of the Zapad exercise?

The Baltic States are small states on the periphery of Europe, which is why the support of allies and the confidence that they will not be left alone in dangerous situations is critical. Exploring the ways in which the Baltic countries were presented in the Western media may point to their current relationship with the allies and security, knowing which steps can be taken in strategic communication to support the image of small states in the desired direction.

1. BEING SMALL IN A CHANGING SECURITY ENVIRONMENT

To this day, there is no clear definition to what constitutes a small state. Thorhallsson and Steinsson (2017) argue that small states could be defined based on the combination of resources and capabilities, especially lack of those which define the extent of their power and influence. From this point of view, small states could be defined based on different quantitative indicators – size of its population, territory, economy (GDP) or its military (Ingebritsen, Neumann & Gstöhl, 2004; Antola, 2002, pp 71). It is obvious that small states' physical resources such as economic wealth, military power, etc. are limited, making them usually the weak actor in international relations.

However, the understanding of the security environment has changed rapidly during the last decades. Realism as a theoretical approach, which dominated decades ago is not capable of explaining the changes in the field today. The emergence of informational, cultural and social factors and their increasing importance is the main reason this study emanates from the constructivist perspective, which emphasizes the importance of ideas, identity and interaction (Agius, 2016, pp 50). Nowadays, security and defence are often seen as social constructs that are influenced by the social, historical and political context.

Fox (2006, pp 40) argues that as big states are usually special due to their great military power, achieving objectives through violence is only one measure of political power. She describes other ways to gain success, which are ideological and diplomatic measures that help to strengthen small states and keep good relations with selected allies (Fox, 2006, pp 40). Thorhallsson and Steinsson (2017) agree with that view saying that small states can compensate the shortages that their smallness causes by choosing the right strategies. Therefore, it is necessary to discuss whether these environmental changes offer new opportunities and give more power to small states. Security and defence have become a very broad study area (Bailes & Rickli, 2014), reaching out from the boundaries of traditional security and defence measures.

The three Baltic states share a border with the Russian Federation, which is regarded to be the greatest threat to their independence (Veebel, 2018; Vaicekauskaitė, 2018; Bailes, 2013). When it comes to the identity, culture and history of the three Baltic States, it is not surprising that they have a mutually shared understanding of the Russian Federation being a threat to the region. It is obvious that the Russian Federation's Zapad-2017 military exercise was aimed at sending a communicative message. The same was intended by the NATO alliance who were actively present in the Baltics and other states in the area that were meant to deter its adversary.

1.1. PURPOSEFUL STRATEGY AND PURPOSEFUL COMMUNICATION

Before discussing the aspects that make a communication strategic, it is crucial to discuss what a strategy actually is. As the security environment changes, there is a need to adapt the strategic thinking to suit the new conditions. Bailes (2009) explains that strategy provides the starting point or foundation from which more detailed, local, and often more flexible 'tactical' actions can proceed. But as the security environment changes and becomes much broader than usual (by combining social, cultural and informational aspects as well), the strategies need to look beyond their traditional borders. When it comes to the public sector, Geoff Mulgan (2009) writes that effective strategies must relate to every part of society. Strategies that belong only to ministries, management, or the strategy unit are doomed to fail. Just like strategies of one function (eg, finance or IT) (Mulgan, 2009, p. 4). Cornish (2011) notes that effective strategic communication cannot be achieved through a solid, discrete, centralised structure, or through any strategic communications department. Success requires a common strategic communication mindset, which should be integrated at all levels: state's strategy, national policy, organisation and department. Therefore, developing a strategic communication mindset and agile network-based approach can be seen as a challenge for states. And here, small administrations could have an advantage.

There are different strategies that small states can choose to secure their existence. Long (2016) defines three strategies that help states to increase their influence:

- **Particular-intrinsic power** considers the means that are intrinsic to the state. For example Bailes (2009) writes about national power and authority, which could be based on some niche-knowledge. This kind of knowledge makes a state valuable to its allies, it helps to collect know-how and increase competence in some field (Bailes, 2009). When a state has a niche-knowledge, it is a deep expertise in some field that is increasingly important to other countries and not easy to replace. Achieving this expertise usually takes investments and resources, therefore it has to be a strategic choice of a state. Due to the lack of diplomatic resources, lack of expertise and consolidation of structural power, small states should focus on the policy sectors that are important to them or where they are most likely to benefit (Thorhallsson & Steinsson, 2017).

- **Collective power** means the relationships with allies. This means that partnerships with international organisations, big or other small states could help to have an impact that is too difficult for one small state to achieve. Bailes (2009) sees two main strategic directions – partnership with a powerful country or partnership with group(s) that have collective power and influence. In the case of the Baltic States, deterrence activities are closely linked to NATO. Viljar Veebel (2018), a research fellow at the Baltic Defense College explains that since NATO's common strategy is deterrence, it should be reflected in its strategic communications. It gives Baltic States a chance to communicate themselves as a part of a strong alliance and therefore it is in the interest of small states that NATO would seem strong.

  The influence and security of small states in the international system can also be enhanced by cooperation with "like-minded" or other small states (Bailes, 2009; Jurkynas, 2007). Cooperation with neighbors can change the country's image and mitigate the effect of smallness, as well as ensure that the special interests of small countries are not ignored (Jurkynas, 2007). At the same time, Thorhallsson and Steinsson (2017) point out that sometimes small countries may have different interests, which makes it difficult to form alliances with each other to balance big powers. Vaicekauskaitė (2017) agrees with this statement and points out that small countries may have similar characteristics, but this does not mean that they share similar foreign policy interests. However, it is also known that the Baltic States share

security threats (Veebel, 2018; Vaicekauskaitė, 2018; Bailes, 2013), which should make their cooperation successful.

- **Derivative power** (Long, 2016) includes infomational activities such as campaigns and lobbying, and strategic communication could be seen as a measure of derivative power. Handel (2006, lk 190) explains that derivative power can be seen as a way for a weak state to achieve its objectives by manipulating the strong powers. He says that weak states are dependent on attraction to other states. That is why he thinks it's the most dangerous for a small state to be isolated from the international system or to get involved in a power-play with a powerful country that could preclude its relationships and interaction with other states (Handel, 2006, lk 190).

There is much that a small state could do to support its chosen path by strategic communication, and therefore increase its derivative power. Thorhallsson and Steinsson (2017) addressed the importance of the image of a small country in its security. They argue that the small country benefits from a neutral and peaceful image. Likewise, small countries can increase soft power through their attractive culture and values. Soft power is the ability of a state to make others want what it wants through temptation and seduction (Nye, 2004). This is particularly important for a small country that is unable to compete with the great powers by means of 'hard power'. However, this appeal is enhanced by the media, which helps to convey these values globally and contributes to the formation of other societies' perceptions of the country.

Therefore, achieving the desired image and reaching a common understanding requires effort from the small state itself, because meaning cannot be created without communication (co-construction of meaning) (Benoit et al., 2015, p. 7). These days journalists have limitations of time and amount of content, which means they have to find the events with the most news value and present them through certain journalistic norms (Ayalon, Popovich & Yarchi, 2016). But it can be argued that state's spokepersons' own messages are one of these bits of information that help to formulate the outcome.

2. ZAPAD AS A PHENOMENA OF INTERNATIONAL NEWS VALUE

From time to time, there are events that bring more international media attention to the Baltic States. One of those was the Russian Federation's Zapad-2017 military exercise. Zapad military excercises date back to the cold war when it was first conducted as a cooperation between the Soviet Union and other Warsaw Pact members. It is one of four military excercises which the Russian Federation conducts in a cycle of four years in four strategic areas: Zapad exercise in the west district, Vostok in the east, Kavkaz in the south and Tsentr in the north (Sazonov & Ventsel, 2018; Stoicescu, 2017; Heuser, et al., 2018, lk 5; Wilk, 2017).

According to Suhhankin (2017), four main conclusions can be made based on the surface of Zapad, one of which was the use of the exercise as an information weapon. He acknowledges that the Russian Federation achieved its main propagandistic objective already before the beginning of Zapad-2017, because it's skilful information manipulation and distortion made it possible to sow the doubts that spread panic in the West (Suhhankin, 2017). Ventsel et al. (2018a) argue that two functions can be distinguished when it comes to spreading fear in the information environment. First, it was intended to create „information fog", which aimed to create confusion among the audience. This was done by manipulative and vague messages, opaque data and attempts to ridicule the West's speculations regarding the size of the Zapad exercise. Constant repetition of such messages led the media to believe that the Russian Federation was hiding its true military capability. The second function aimed at convincing the audience that the Western media (EU and NATO spokepersons) were the ones spreading fear and paranoia and were the generators of such information hazards. They conclude that Russia succeeded in creating an image of a dreaded and militant enemy in the Western media, and the resulting sense of danger in turn reproduced the discourse on Russian military power. (Ventsel, et al., 2018a)

Zapad-2017 gave an opportunity to study the ways the Baltic States were presented in the Western media and see what could be learned from the messages that were presented in the media reports in the Western online

news media. The aim of this study was to examine how the Baltic States were presented in the Western media in the context of the Zapad-2017 excercise and indicate lessons for strategic communication. The research problem was formulated:

How were the Baltic States presented in the Western media in 2017 in the context of the Zapad exercise?

To find an answer to this research problem, three research questions were posed:

1. What was the main content of the messages presented in Western online media about the Baltic States and, as a result, the overall image of the Baltic States?

2. How did the Baltic States' messages influence this image?

3. What were the main lessons for the Baltic States in terms of strategic communication?

Therefore, this study attempts to detect the link between the states' strategic communication activities and their outcome in the media. To find an answer to this question, qualitative content analysis of media texts from nine online news portals were used.

3. QUALITATIVE CONTENT ANALYSIS AND SELECTION OF ARTICLES

In this study, a qualitative content analysis was used as a data analysis method. A qualitative approach enables a phenomenon to be described, to understand the processes within it, show the different views, motivations and experiences of the participants and explain the meaning attached to these experiences (Forman & Damschroder, 2007). Qualitative text analysis is a form of analysis in which understanding and interpreting text plays a much larger role than in classical content analysis, which is limited to listing "visible" content (Kuckartz, 2014, p. 33). It explores aspects of the texts that quantitative analytical techniques do not reach. Kuckartz (2014, pp. 30-32) sees quantitative analysis as an important part of qualitative analysis rather than an alternative to it, and therefore quantitative analysis can be considered as the first step of qualitative analysis.

Media texts from nine Western news media online portals were studied: Reuters, The Guardian, Politico, BBC, Bloomberg, EU Observer, Foreign Policy, The New York Times and The Washington Post. These were chosen as they are widely spread and based in the United States, UK or Brussels, which can be regarded as having an important connection to the Baltic States' allies and security. First, the articles were searched with the keyword „Zapad" and 174 results were found. Then, articles which mentioned the Baltic States, the region or one of these states were mapped. The total number of analysed articles was 96 and these were published in 2017 between February 9th and December 27th.

Then, three phases were used in the coding process: immersion, reduction and interpretation (Forman & Damschroder, 2007). In the first step, the researcher read and examined the research material and got an overview of the "whole" before organising it into the units. In the second phase, a systematic approach to data processing was developed. The most important analysis units were picked and organised regarding the research question. The study used both deductive and inductive categories. The analysis units of the study were the paragraphs of the media

texts that mentioned the Baltic States. These units were assigned to five categories:

- **Messages assigned to the Baltic States**, which included four separate sub-categories (Baltic States, Estonia, Latvia, Lithuania). A distinction was made here between the comments of the "spokepersons" of these countries and the presentation of each individual country. Spokepersons are people who are quoted (regardless of their role) or attributed views (such as "person said" or "person thought") in web texts.

- **The Baltic States' context**. Studies how the Baltic States were described without referring to any country's messages. As the paper explores ways of presenting the Baltic States, the reactions and actions attributed to them were also taken into account.

- **Security environment affecting the Baltic countries.** This category contained both deductive and inductive codes. The aim was to find out to what extent some aspects of the theory (including deterrence, unity) were presented in these presentations. However, it was not limited to deductive subcategories and codes, since for the purpose of the research it was necessary to identify other aspects that were presented in the media texts.

- **Zapad 2017**. The description of the major exercise was grouped into one category. This category was chosen because many speculations about Zapad's possible consequences and the aims of the event were spread in the studied texts.

- **Other context**. The fourth category contained parts of the broader context which were not directly related to the Baltic States and as such were not analysed in depth.

At this stage, an initial coding guide with deductive categories, subcategories and codes was developed. This coding guide was developed by analysing 27 articles (3 articles from each portal) and inductive codes were added. After that, all the articles were coded by the final coding guide.

The last phase involved analysing, interpreting, and synthesizing code reports and memos to complete the results. Afterwards, the patterns

that emerged during the analysis were explained, noteworthy results highlighted, and placed in the theoretical framework. The Nvivo 11 Pro qualitative data analysis programme was used to conduct the analysis.

4. ESTONIA, LATVIA AND LITHUANIA IN THE WESTERN ONLINE NEWS MEDIA

4.1 RESULTS

The Baltic States were named in 96 articles and these texts were the objects of this analysis. In total, 174 articles mentioned Zapad, and the Baltic States were presented in more than a half of these texts. The analysed texts were published in 2017 between February 9th and December 27th. As expected, most media texts were released in September 2017. During the Zapad event alone (14.09.2017-20.09.2017) 21 media texts were published. It is one more than after the event (21.09-27.12.2017). The media interest grew in July and decreased signficantly after November 2017. The first analysed media text was published in February 2017 after which the media interest grew gradually. As it can be seen from the following table, most of the texts were published before Zapad (09.02-13.09.2017).

TABLE 1. The number of analysed media texts by publication and period

Portal	Before Zapad	During Zapad	After Zapad	Total
Reuters	25	4	6	35
The Guardian	6	2	0	8
Politico	6	2	3	11
BBC	1	3	0	4
Bloomberg	1	1	2	4
EU Observer	6	1	1	8
Foreign Policy	5	1	3	9
The New York Times	3	2	1	6
The Washington Post	2	5	4	11
Total	**55**	**21**	**20**	**96**

Most of the articles (35) were from the Reuters online portal. This was followed by Politico and The Washington Post, each of which published 11 articles on the Zapad exercise that mentioned the Baltic States.

Of the **Estonian** spokespersons, the defence ministers were quoted the most: in 6 articles in total. Five of the quotes belonged to Margus Tsahkna (Estonian Minister of Defense from 11.2016 to 06.2017), one to Jüri Luik (Estonian Minister of Defense from 06.2017). The comments of Prime Minister Jüri Ratas were published in 3 articles, while the other spokesmen were included in one article, including Permanent Secretary of the Ministry of Defense Kristjan Prikk, and Commanders of the Defense Forces at the time Riho Terras and Hannes Hanso. One article in The Guardian presented the assessments of civilians and four people explained the situation. On one occasion, the comments of Estonian President Toomas Hendrik Ilves were also published. Estonia was mostly mentioned in connection with the presence of allied forces in the area (8 texts) and international events (7 texts). The two largely overlapped: allies' representatives' visits to Estonia on several occasions, which involved visiting troops that were located in Estonia (Jens Stoltenberg visiting British troops, Florence Parly visiting French troops). Estonia's (and Lithuania's) participation in the Aurora exercise was also noted.

Latvia was presented mostly in two contexts: as a state in the Zapad region (with Lithuania) and hybrid threats. Comments of Foreign Minister Edgars Rinkēvičs were presented in six articles, which focused mainly on the elements of hybrid warfare. Statements of the Latvian Minister of Defense Janis Garisons were presented on two occasions, which focused on Russia's overall ability to wage a hybrid war with the West. In addition, Vice Chairman of the National Security Committee of the Latvian Parliament Karlis Serzants and President Raimonds Vejonis were quoted each in one article. On one occasion, an impersonal reference was made to Latvian security officials and three civilians' opinions were asked about Zapad.

Of the three Baltic countries, **Lithuania** was the most represented in the Western media in the Zapad context. An analysis of the messages from Lithuanian officials revealed that two persons - or the Lithuanian Defense Minister Raimundas Karoblis and President Dalia Grybauskaite – were presented the most. Lithuanian Minister of Defense Raimundas Karoblis quotes were used in 7 articles, stressing the potential for conflict and referring to Zapad's offensive nature. He clearly emphasized expectations for the allies' response and often referred to unity. President Dalia Grybauskaite was quoted in five articles and one interview. She

also saw Zapad as an offensive exercise against its neighbors, which was a consistent message of the other Baltic States and their allies. The President often referred to unity and called on NATO to use additional security measures in the region. The quotes of the Lithuanian Minister of the Interior Eimutis Misiunas appeared in two articles in which he explained the construction of the Lithuanian border. In addition, the following people were presented: Commander of the Lithuanian Land Forces Maj Gen Valdemaras Rupšys, Vice-Minister of National Defence Vytautas Umbrasas, Head of the Liberal Movement in the Lithuanian Parliament Eugenijus Gentvilas, Spokesman for the Lithuanian Border Guard Service Rokas Pukinsas and Lithuanian Foreign Minister Linas Antanas Linkevicius. Their quotes were each featured in a single article.

4.2 DISCUSSION

As stated in the last chapther, three research questions were formulated. The overview of the main findings are presented regarding each of these research questions.

The first research question was: *What was the main content of the messages presented in the Western online media about the Baltic States and, as a result, the overall image of the Baltic States?*

Over a third of all articles had messages indicating to deterrence and/or unity of the Western alliance. There is a thin line between deterrence and unity, but in this study, military steps were regarded as a deterrence and unity was described by words and opinions regarding the allies' actions, plans and promises. It can be said that Zapad-2017 was taken seriously by NATO and the US, counteractions were described in the media during the whole year, not only during the period of the Zapad exercise. This shows an effort to show themselves as active and prepared actors.

The Baltic States were presented in the Western media as small states that are strongly supported by the NATO alliance and the United States, and who cooperate actively with other western states. As mentioned previously, international cooperation helps to relieve the small state effect and different forms of cooperation were often presented in media texts.

Article 5, which refers to the collective defence, and allies' presence in the Baltics (e.g international drills, visits, events) were often mentioned:

> „U.S. Vice President Mike Pence on Monday assured the Baltic states of U.S. support if they faced aggression from Russia, telling them that Washington firmly backs NATO's doctrine of collective defense." (Reuters, 31.07.2017)

Although the Baltic States were strongly indicated as partners and part of an alliance, the Russian Federation was presented as a threat to the Baltics which has previously interfered and will probably do so in the future. Mostly the threat was explained through its previous actions in Ukraine and Crimea. It is important to note that this can be misleading as it indicates that a similar scenario could happen to the Baltic States. It should be kept in mind that the security environment of these countries is different, perhaps the most obvious would be membership of the NATO alliance. Also, the Russian Federation's activities against the Baltic States were mentioned, which supported the Baltic concerns during the exercise period. Some of the media texts mentioned the Baltic States as border states or previous Soviet states and their history was briefly presented. Briefing the audience about the history of the Baltic States and their relationships with the Russian Federation and Soviet Union could support the mutual understanding of the Russian Federation as the main security threat to Baltic States. For example, when discussing the situation of Estonia, Politico stated:

> „Situated across a 200-mile long border with Russia, Estonia — invaded by the Soviet Union in World War II and occupied for 70 years — is seen by strategists as a likely target for Russian aggression that could test the NATO alliance" (Politico, 29.07.2017)

As mentioned previously, the Russian Federation's skillful information manipulation lead to doubts which spread panic in the West. Analysing media texts lead to the conclusion that many different scenarios spread about the possible outcome of the exercise. On one hand it could be seen as spreading doubts and fear. On the other hand, it could help to conduct deterrence activities: discussing different possible outcomes means that there are fewer opportunities for the adversary to suprise. Mostly, it was suspected that the Russian Federation would leave military equipment

and troops in the area (without discussing where this could lead). For example, the Lithuanian defence minister at the time Raimundas Karoblis explained the situation:

> „Lithuania's defence minister, Raimundas Karoblis, suggested there was even a risk of the drill triggering a conflict or being used as cover to leave behind troops in Belarus. "We can't be totally calm. There is a large foreign army massed next to Lithuanian territory," he told Reuters." (Reuters, 13.09.2017)

Also, some of the Baltic weak spots were mentioned (Suwalki corridor, big Russian-speaking minorities). It could be regarded positive to the Baltic States that potential misbehaviour by the Russian Federation was mainly mentioned by indicating to its previous actions not as an outcome of a weakness of the small Baltic States. Some of the weaknesses of the Baltic States were mentioned, such as a need for an airforce or the possibility to influence russian minorities. Also, the need for additional forces was strongly suggested by Lithuanian spokepersons, which on one side could influence the alliance to bring its forces to the area, but just as well show the Baltics as small states in need. It is clear that chosen communication activities should consider both sides and aim towards the outcomes that are strategically more beneficial and important at some point in time.

All in all, there was no doubt that the Baltic States were seen as part of the alliance, but it would be crucial that the whole alliance was presented as strong and united. That's where some of the Baltic messages could be improved. Indicating to NATO as to a third party who makes decisions and who is hoped to bring forces to the eastern front could send a message that these topics haven't been agreed upon yet. Also, some „what if..." scenarios were presented which discussed the outcomes of a real attack and the alliance's potential inability to actually react in the event of a real attack. However, these discussions remained hypothetical and it can be regarded as a part of the information environment, which is not controlled by any state or alliance itself.

The second research question was: *How did the Baltic States' messages influence this image?*

The three Baltic States were presented in the Western media in different ways. It is understandable, as although small states have many similar qualities, they often pursue different interests and objectives. Messages of all three supported the presentation of the Baltic States being a part of NATO. However, each of the Baltic States messages had a different focus and way of expression. It should be pointed out that this article is concerned with media presentations, not the states' actual strategies and aims. This means that these presentations were shaped by journalistic interpretations.

Estonia's possible objective was to present itself as a calm and rational small state. This was pursued by very straightforward and clear messages, which were mostly free of emotions and very similar to the messages of the alliance:

> „The prime minister of Estonia, Jüri Ratas, who joined Stoltenberg at the base in Tapa [--]said: "I would like to say that we are concerned about the nature and lack of transparency of the exercise. Our attitude remains cool and confident. Along with our allies we will monitor the exercise very closely and remain ready for every situation." (The Guardian, 06.09.2017)

With only few exeptions, Estonia's spokepersons remained calm and did not speculate over possible scenarios (except the possibility of the Russian Federation leaving its troops in the area). Estonia's spokepersons focused on observing the drill and being prepared in case any dangerous events should take place. Just like other Baltic States, Estonia's spokepersons indicated the need for the allies presence in the area and these expectations were explained to be „a logical step" regarding the previous cooperation and today's security environment without indicating their own weaknesses, as Estonia's defence minister at that time, Jüri Luik explained:

> "Similar to having an armored British battalion here, it would be equally logical to have anti-aircraft assets," Luik, a 50-year-old career diplomat, said in an interview in the capital, Tallinn. "It doesn't add any drama. It's rather just an element of deterrence." (Bloomberg, 13.07.2017)

Latvia's spokepersons strongly focused on different hybrid threats. Just as explained earlier, focusing on a niche-topic could increase a small states soft power in the international arena as it gives a chance to raise its competences and know-how on some important topic, and makes a small state more „useful" to its alliances. There were comments that pointed out the the Russian Federation's activities in hybrid warfare (e.g disturbing phone lines or spreading fake news). As was said in the statement of Latvia's Ministry of Foreign Affairs:

> „During the Zapad 2017 exercise, we cannot rule out activities involving hybrid threats directed against the Baltic States, including aggressive propaganda and fake news, manipulations with public opinion, cyber-attacks and others." (Politico, 12.09.2017)

It can be said that the niche of hybrid threat suits the overall context well. Latvia's spokepersons sometimes presented their ideas vaguely and at times they weren't based on official statements:

> „„Our authorities are analysing a pattern of communications disruption that appears to have originated during the Zapad exercise against Öland Island, with some direct impact to Latvia," Rinkevics said. [--] Rinkevics said Latvian authorities are also examining possible Russian involvement in a Sept. 13 outage of Latvia's emergency phone hotline. Nothing has yet been proved, he said." (The Washington Post, 05.10.2017)

As pointed out earlier, during risky situations it is important to keep messages clear and well grounded, and to avoid them being stated too early (not agreed upon with allies or without having an official confirmation).

Lithuania can be regarded as very clear in its messages. As from the Baltic States Lihtuania was geographically the closest to the area of the exercise, Lithuania also expressed the greatest need for allies to be present in the region:

> „Lithuanian president Dalia Grybauskaite has urged Nato to beef up security in its Baltic allies ahead of a mass-scale Russian drill in September that is to simulate an invasion. "We are worried about the upcoming Zapad 2017 exercise, which will deploy a very large and

> aggressive force [on our borders] that will very demonstrably be preparing for a war with the West," she said in Riga on Friday, Reuters reports." (EU Observer, 10.02.2017)

Lithuanian speakers discussed the most likely results of Zapad from the other Baltic countries, sometimes highlighting the weaknesses of the Baltic countries and expressed their dependence on allies. The speeches of the Lithuanian speakers sometimes gave the impression that NATO is being spoken of as a third party, which could indicate the country's exclusion from decision-making processes or its inability to contribute to joint decision-making:

> „„We expect so," defense minister Raimundas Karoblis told Reuters when asked if he saw an agreement shaping up for the NATO summit in 2018. "Air defense is one of the issues which we need to address. We also need to look at other domains, like NATO command structure reform, we need to move forward on all of these aspects," he said, also calling for NATO to strengthen maritime defenses in the Baltics. [--] Karoblis said exercises should be considered by NATO after Russia's Zapad war games unnerved the West in September." (Reuters, 07.11.2017)

In general, it can be argued that the communication strategy chosen by Lithuania demonstrated the effectiveness of the strategic communication process and its messages contributed most to the general Baltic States' image. At the same time, this study can not make any definite conclusions because this study does not establish a cause-effect relationship between what was intended and what was presented in the information environment.

The third reserach question was: *What were the main lessons for the Baltic States in terms of strategic communication?*

The study provided an overview of the presentation of the Baltic States in the Western media in the context of the Russian Federation's military exercise Zapad-2017. Also, it was discussed how the messages of the three Baltic States spokepersons' contributed to these presentations. Based on the theoretical and empirical parts of this study, there are some aspects

that could be regarded important in organising and carrying out strategic communication in a small state.

First and foremost, there is a need to **know your adversary**. The deep knowledge of the adversary is important for multiple reasons. Perhaps the most important one is to coordinate one's messages in a way they would not contribute to the achievement of your opponent's goals. For example, the Russian Federation's objective is to be regarded as a threat and it wants to be seen as strong and dangerous. Therefore, the Baltic States should try not to frame the Russian Federation *this way*, but perhaps frame its actions through its dishonest behaviour instead. On the other hand, explaining the Baltic States' relationship with the Russian Federation and it's behaviour could improve allies' mutual understanding about the state as a security threat.

It is not always possible nor necessary to avoid talking about small states' weaknesses. However, discussing different voids in defence could make a small state seem weak and needy. Instead, it would be beneficial to **concentrate on your strengths** and the ways it deals with different security threats. This could send a message that a small state is actively preparing for risks that its environment provides and it is a strong partner to other states in the alliance. As discussed previously, although small states may be considered weak regarding traditional means of war, these are not the only important aspects in the changing security environment. As seen from the analysis of the media texts, worrying about weaknesses could lead to the journalistic interpretation of negative emotions (fear, concern, anxiety) which contradicted the messages of the NATO alliance, which tried to sound calm and confident.

The study presented that NATO's main messages included being **confident, but prepared**. To contribute to the unity of the alliance, the small states should keep these attributes as a part of their messages as well. This helps to frame themselves as part of a strong alliance.

As discussed before, the general security environment is changing and the problems that the states face have become wicked. Therefore, there is a need to lose the traditional boundaries between different institutions because there are increasing number of topics that can be regarded important in a state's defence and security. There is an ineluctable need to

coordinate strategic communication as a network. In order to respond to modern challenges, successful strategic communication needs to move beyond existing silos. As pointed out previously, effective strategies must relate to every part of society. Strategies that belong only to ministries, management, or the strategy unit are doomed to fail. Just like strategies where only one function dominates (eg, finance or IT). It could be necessary to develop a strategic communication mindset across state institutions that would help public institutions network and strengthen the state's position in each key area. There is a need for this network-based approach to become international, especially for a small state.

It could become helpful to **prioritise the main messages between the Baltic States.** Obviously, three small states may have different strategies, but the objective is usually the same – to keep the region safe. Repeating and emphasising the most important messages increases the probability of them being represented in the media. When these messages are expressed simply, they are better understood and more often reused in media texts.

If possible, the Baltic States should find a common **niche-knowledge** that could be supported by strategic communication and would help them to increase their power on the international stage. Although, generally it should be considered thoroughly whether the context is right to communicate a niche topic. Hybrid threats as a niche may have suited well to the Zapad context, but forcing the niche-related messages can contribute to the creation of information fog, which could make it harder to achieve goals set with communication activities. Also, it should be kept in mind that the niche-topic is something that the state has a strong competence and knowledge in. This means that raising the expertise presupposes investment of time and resources, therefore should be chosen strategically.

And last but not least, it is crucial to **prepare early** for events like Zapad-2017. Media interest towards the exercise could be seen in the beginning of the year. It would be much easier to agree upon messages and forming them to suit the state's strategic objectives when it is done in a timely manner.

All in all, the small states should contribute to improving the relationships with chosen allies and sending messages that they are part of a strong institution. Small states are usually more influenced by their environment than big ones, but that does not mean that they can not concentrate on building themselves to become strong and agile when dealing with suchrisks. After all, adversaries can change over time, but the objective of staying alive will never change.

5. CONCLUSION

The purpose of this study was to examine how the Baltic States were presented in the Western media in the context of the Zapad-2017 excercise and indicate lessons for strategic communication. The study points out seven suggestions to the Baltic States to consider in their future strategic communication processes.

It can be argued that Lithuania's messages contributed most to the general Baltic States' image, which indicates that the state could have coordinated it's messages successfully. Although it can not be stated in full certainty because the study focused only on media texts and did not analyse these states' actual communication strategies. It shows that the Baltic States should consider a mutual media communication strategy as otherwise the aims of one state could be presented as the others as well. It should be pointed out that Lithuania was the one whose messages were presented the most in quantitative terms as well, which contributed to gaining the desired image.

The three Baltic States certainly have different communication strategies, but the overall objective of their strategies are usually the same – to keep the region safe. There were several similar messages in the three states media presentations. The most evident of these were hybrid threats which could have potential in becoming the Baltic States' mutual niche topic. Also, unity with the allies and the desire to have allies presented in the area were discussed a lot and these messages were expressed in a different manner. This shows that actors can express themselves in a different way to gain similar goals. Repeating and emphasising the most important messages and expressing them in a simple, catchy manner increases the probability of them being represented in the media.

It should be stressed that this study can not make any definite conclusions because it does not establish a cause-effect relationship between what was intended and what was presented. But it unveils the ways the presentation is shaped in the media environment and what the outcome of the communication activities conducted during the Zapad exercise in 2017 was.

ACKNOWLEDGEMENTS

Thank you Matthew Crandall (Tallinn University) and Diana Marnot (Estonian Academy of Security Sciences) for supervising my master's thesis that made this article possible.

Contact:

Kerli Onno
E-mail: kerlionno@gmail.com

REFERENCES AND SOURCES

Agius, C., 2016. Social Constructivism. Book: A. Collins, *Contemporary security studies*. Oxford university press.

Antola, E., 2002. The future of small states in the EU. *European integration in the 21st century: Unity in diversity*, pp 69-85.

Ayalon, A., Popovich, E. and Yarchi, M., 2016. From warfare to imagefare: How states should manage asymmetric conflicts with extensive media coverage. *Terrorism and Political violence*, 28(2), pp 254-273.

Bailes, A.J.K., 2009. Does a small state need a strategy? *Centre for small state studies Publication series*. University of Iceland, 2.

Bailes, A.J. and Rickli, J.M., 2014. Small states, survival and strategy. In: *Small States and International Security*. Routledge, pp 52-71.

Bailes, Alyson JK (ed) Defence and Security for the small: Perspectives from the Baltic States. Raimonds Rublovskis, Margarita Šešelgyte, Riina Kaljurand. Centre for Small State Studies, Institute of International Affairs, 2013.

Bennett, W.L., Paletz, D.L. (ed.-s), 1994. *Taken by storm: The media, public opinion, and US foreign policy in the Gulf War*. University of Chicago Press.

Benoit, W., Holtzhausen, D., Zerfass, A., 2015. Image repair theory in the context of strategic communication. *The Routledge handbook of strategic communication*, pp 303-311.

Cornish, P., Lindley-French, J., Yorke, C., 2011. *Strategic communications and national strategy*. Chatham House, The Royal Institute of International Affairs. [Online source] Available from: https://www.chathamhouse.org/sites/default/files/r0911es%E2%80%93stratcomms.pdf [Accessed 10.01.2019].

Forman, J., Damschroder, L., 2007. Qualitative content analysis. In: *Empirical methods for bioethics: A primer*. Emerald Group Publishing Limited, pp 39-62.

Fox, A., 2006. The Power of Small States : Diplomacy in World War II. In: *Small States in International Relations*.

Handel, M. (2006). Weak States in the International System. In: *Small states in international relations*. University of Washington Press, pp 149-192.

Heuser, B., Heier, T., Lasconjarias, G., 2018. *Military exercises: Political messaging and strategic impact*. NATO Defense College. [Online source] Available from: http://eprints.gla.ac.uk/165109/1/165109.pdf [Accessed 04.05.2019].

Ingebritsen, C., Neumann, I., Gstöhl, S. (ed.-s), 2006. *Small states in international relations*. University of Washington Press.

Jurkynas, M., 2007. *How deep is your love?: the Baltic brotherhood re-examined*. Institute of International Relations and Political Science, Vilnius University.

Kuckartz, U., 2014. Qualitative Text Analysis: A Guide to Methods. *Practice & Using Software.* Sage, London.

Long, T., 2016. Small states, great power? Gaining influence through intrinsic, derivative, and collective power. *International studies review*, 19(2), pp 185-205.

Mulgan, G., 2009. *The art of public strategy: Mobilizing power and knowledge for the common good*. Oxford University Press on Demand.

Naveh, C., 2005. The Role of the Media in Establishing International Security Regimes. *Conflict & Communication*, 4(1).

Nye Jr, J.S., 2004. Soft power. In: *Power in the Global Information Age*. Routledge, pp 76-88.

Sazonov, V., Ventsel, A., 2018. Sõna saateks. Sõjaväeõppus Zapad 2017 Venemaa infosõja kontekstis. *Sõjateadlane (Estonian Journal of Military Studies)*, nr 8, lk 7–15.

Stoicescu, K., 2017. Decoding Zapad-2017 : analysis. International Centre for Defence and Security. September 2017. [Online source] Available from: https://icds.ee/wp-content/uploads/2018/ICDS_Analysis_Decoding_Zapad-2017.pdf [Accessed 05.04.2019].

Suhhankin (2017). Zapad 2017: Mida õppus õieti näitas? Diplomaatia. [Online source] Available from: https://diplomaatia.ee/zapad-2017-mida-oppus-oieti-naitas/ [Accessed 03.03.2019].

Thorhallsson, B., Steinsson, S., 2017. Forthcoming in the Oxford research encyclopedia of foreign policy analysis (post-referee, pre-copyedit version). Small state foreign policy.

Vaicekauskaitė, Ž.M., 2017. Security Strategies of Small States in a Changing World. *Journal on Baltic Security*, 3(2), pp 7-15.

Vaicekauskaitė, Ž.M., 2018. Security strategies in the nordic baltic regioon: towards enhanced regionaal defence cooperation? *Policy brief* , 10. Presented at the conference 'Small States and the New Security Environment at the Nordic House, Reykjavik Iceland.

Veebel, V., 2018. NATO options and dilemmas for deterring Russia in the Baltic States. *Defence Studies*, 18(2), pp 229-251.

Ventsel, A., Hansson, S., Madisson, M.-L., Sazonov, V., 2018a. *Representation of the russian zapad 2017 military exercise in the estonian news media* [Upcoming]. In: Matthew A. Lauder, Anthony Seaboyer (ed.-s) Emerging threats in the information environment: Final report of Research Task

Group 117. NATO Science and Technology Organization, PUB REF NBR (E.G. STO-TR-IST-999), pp. XX-38.

Wanta, W., Golan, G. and Lee, C., 2004. Agenda setting and international news: Media influence on public perceptions of foreign nations. *Journalism & Mass Communication Quarterly*, 81(2), pp 364-377.

Wilk, A., 2017. The Zapad-2017 Exercises: The Information War (for Now). Centre for Eastern Studies (OSW). [Online source] Available from: https://www.osw.waw.pl/en/publikacje/osw-commentary/2017-09-04/zapad-2017-exercises-information-war-now. [Accessed 04.04.2019].

QUOTED ARTICLES

Reuters, 07.11.2017. https://www.reuters.com/article/us-nato-lithuania/lithuania-expects-nato-to-reach-deal-on-baltic-air-shield-idUSKBN1D72LL [Accessed 04.10.2019].

EU Observer, 10.02.2017. https://euobserver.com/tickers/136870 [Accessed 04.10.2019].

The Washington Post, 05.10.2017. https://www.washingtonpost.com/world/europe/latvias-cellphones-stopped-working-russias-war-games-may-be-to-blame/2017/10/05/449162d4-a9d3-11e7-9a98-07140d2eed02_story.html [Accessed 04.10.2019].

Politico, 12.09.2017. https://www.politico.eu/article/eastern-front-zapad-military-exercises-russia-lithuania-belarus/ [Accessed 04.10.2019].

Bloomberg, 13.07.2017. https://www.bloomberg.com/news/articles/2017-07-13/russia-s-nato-neighbor-in-talks-over-anti-aircraft-weapons [Accessed 04.10.2019].

The Guardian, 06.09.2017. https://www.theguardian.com/world/2017/sep/06/nato-russia-belarus-zapad [Accessed 04.10.2019].

Reuters, 13.09.2017. https://af.reuters.com/article/worldNews/idAFKCN1BO1OK [Accessed 04.10.2019].

Politico, 29.07.2017. https://www.politico.com/story/2017/07/29/estonia-russia-us-visits-pence-241098 [Accessed 04.10.2019].

Reuters, 31.07.2017. https://www.reuters.com/article/us-usa-pence-estonia/vp-pence-in-the-baltics-voices-support-for-mutual-defense-in-nato-idUSKBN1AG1G0 [Accessed 04.10.2019].

CYBERSECURITY EDUCATION IN ESTONIA: BUILDING COMPETENCES FOR INTERNAL SECURITY PERSONNEL

Piret Pernik, MA
NATO CCD COE
Researcher

Keywords: cybersecurity and cybercrime curriculum, cybersecurity and cybercrime knowledge, skills, and abilities of law enforcement, the internal security sector

ABSTRACT

Currently there is no formal cybersecurity education for internal security first-responders in Estonia. The Estonian Academy of Security Sciences (EASS) does not provide this education at basic (all students) and advanced (cybercrime investigators) levels. The Estonian government has highlighted the need to improve the cybersecurity competence of mid-level and senior civil servants in the administrative area of the Ministry of the Interior.

In this context, this article gives an overview of cybersecurity formal education and extra-curricular initiatives in Estonia, including those supported by the Ministry of Defence. It further gives a snapshot of the state-of-the-art cybersecurity education in the police academies of Finland, Germany, the Netherlands, and Norway, as well as of other international competence building frameworks. The author recommends several policy solutions in order to improve digital skills, cybersecurity and cybercrime competences of future internal security personnel. The following aspects should be considered in competence building: the existing frameworks, best practices from foreign police universities and academies, and developing closer cooperation with the Estonian Defence Academy, TalTech, and the Ministry of Defence.

INTRODUCTION

The functioning of the Estonian economy and society depends to a large degree on the digital environment. Estonia is a leading country in Europe in public e-services, and is also considered a leader in digital transformation and e-governance. In cybersecurity Estonia ranks fifth globally (International Telecommunication Union, 2018). Digitisation brings to public administrations and private sector companies great socio-economic benefits. It brings efficiencies and cost savings, enhances business transactions. Digital tools that increase transparency and accountability also support the strengthening of democracy by reducing opportunities for corruption.

Emerging technologies, such as artificial intelligence (AI) narrowly defined, bring great opportunities to governments and militaries, as well as for law enforcement agencies. The European law enforcement agencies have begun to use AI systems in order to reinforce their investigative capabilities and strengthen digital evidence (Craglia et. al., 2018). For example, machine learning tools enable more proactive policing to be conducted and improve data analysis and identity checks (European Commission, 2019a).[1] They can aid police to prevent crimes and send out patrols to urban districts where there is more crime, track illicit money flows, predict criminal and terrorist action, identify suspicious behaviour, persons of interest and stolen vehicles, discover criminal patterns, and detect, target and interdict crimes (Ibid, 2019). In Norway and Poland the law enforcement agencies use machine learning tools in order to identify online child exploitation material and monitor disinformation campaigns (Skattor, 2019).

On the flip side, digitisation of almost every aspect of society brings greater cybersecurity risks. Negative tendencies of new technologies

[1] According to the definition provided by the European Commission AI refers to a machine or algorithm that observes and learns from its environment, and based on this knowledge and experience, can take intelligent actions or propose decisions. Common AI technologies are machine learning, data science, robotics, internet of things and use of big data (European Commission, 2019a). The term AI refers to a constellation of AI-related technologies of which four are the most crucial: more narrowly defined AI, machine learning, big data and Internet of Things (Wright, 2018).

illustrated by the growth of cybercrime and more complex, coercive and destructive cyber-attacks that have in recent years inflicted costs worth billions of euros (for example notPetya malware in June 2018). Cyber-attacks threaten national security and public order. For example, in September 2019 Iran used a swarm of drones to attack an oil refinery in Saudi-Arabia, which caused loss of production and affected global oil prices (Kirkpatrick and Hubbard, 2019). Drone exploit toolkits and malware for smart home devices are already traded on the digital dark market, while designer psychedelic drugs, which are not designated as illegal, are sold in internet forums (McAfee, 2018; Silberglitt, et. al., 2015). Criminals will be able to hack personal medical devices (such as pacemakers, heart rate and blood glucose monitors among others) and produce guns with 3D printers (Silberglitt, et. al., 2015). Drones can also be used for smuggling and espionage, autonomous cars can be hijacked or used for launching cyber-attacks, and automated tools are used for software vulnerability scanning.

AI tools will enable cybercriminals to become more agile and better in circumventing protections (McAfee, 2018). Technological development and digitisation (for example employment of 5G and Internet of Things) will expand both cyber-attack vectors and surface. New vulnerabilities have already emerged from storing huge amounts of data in clouds and from Internet of Things devices which commonly lack cybersecurity standards. The complex ICT supply chain with third-party-dependencies is increasingly difficult to secure against software and hardware vulnerabilities, and cyber-attacks through a long chain of vendors and subcontractors. Many scholars and industry experts have assessed that in the coming years cybercriminals and adversary nation states and groups supported by them will use various emerging technologies to commit new crimes with the aim to impair national security.[2]

[2] Game-changing (also called emerging and disruptive) technologies include autonomous devices and systems, artificial intelligence and machine learning, advanced robotics, virtual and augmented reality, blockchain/distributed ledger technologies, Internet of Things, additive manufacturing (also called advanced manufacturing and 3D printing), quantum computing, data storage technologies such as cloud, human-machine interface, telecommunication technologies such as 5G, biotechnologies, privacy-enhancing and anonymisation technologies, etc.

In this context this article discusses introducing digital skills, cybersecurity and cybercrime study themes into the internal security formal education system. The main research questions are the following:

- What is the status of formal (primary, secondary and tertiary level) cybersecurity education and extra-curricular training in Estonia?
- How can the internal security personnel's competences be efficiently and effectively increased by the existing extra-curricular activities? How can the EASS cooperate with other education providers in Estonia in order to benefit from the existing formal and extra-curricular offer?
- What can Estonia learn from best practices in other countries and international organisations in order to develop a basic and advanced formal education curriculum for internal security personnel?
- What type of courses should the EASS develop on its own and which international courses are available for EASS cadets and students, as well as the internal security personnel?

The central research objective is to identify, based on the document analysis and expert opinions, a number of study themes to be included as of autumn 2020 into vocational and bachelor study programmes of the Estonian Academy of Security Sciences (EASS). In order to achieve this research objective and answer the above research questions the author conducted desk-research comprising of academic and specialist literature reviews, existing curricula, competence building frameworks and other relevant documentation. The author conducted several face-to-face and email interviews with domestic and foreign subject matter experts. Insights were also gathered from two working meetings with subject matter experts in Estonia, and an international working meeting in Finland.[3]

[3] Two working meetings were held and face-to-face and email interviews were conducted by the author between February and September 2019. Three in-person interviews were conducted with teaching personnel from police academies in Finland and Germany, and from TalTech in Estonia, which were followed up by a number of email interviews. The author took notes from discussions at the working meetings with experts from the Police and Border Guard Board and the EASS, and incorporated these insights into research results. The best practices from Finland, Germany, the Netherlands and Norway were collected from a literature review, during the interviews and in a working meeting in April 2019 in Tampere.

The article gives a snapshot of the existing cybersecurity education in the police academies of Finland, Germany, the Netherlands and Norway.[4] It does not aim to present representative research results of the current best practices in Europe, but rather it outlines the Estonian approach comparing it with other countries and international-level activities in Europe.[5]

[4] The police academies in the four countries were chosen because they had recently introduced cybersecurity into the curriculum, and the Estonian Academy of Security Sciences had close working relationships with them. This enabled the author to learn from recent experience and gave access to subject matter experts who were responsible for the matter. In the future research, best practices from other police academies (for example, in the UK, US, other Nordic countries, Latvia and Lithuania) could be analysed as the current overview four countries are not representative of the trans-Atlantic, European or Nordic-Baltic best practices. The scope of the current research did not enable including more countries.

[5] This article presents only preliminary results from a longer research project. At this stage of the project data was gathered with qualitative methods (literature and document reviews, interviews and meetings) and results have not been validated with other qualitative and quantitative research methods (such as questionnaires, focus groups). The following phases of the research project should include validation.

1. CYBERCRIME PHENOMENA AND CYBERCRIME COMPETENCE OF CIVIL SERVANTS

First responders at a crime scene must have basic knowledge of cybercrime investigations in order to be able to detect, target and interdict crimes.[6] Cybercrime phenomena can be divided for legal discussion purposes into two categories: cyber-enabled and cyber-dependent crime. However, it is expected that in the near future most crime investigations will have some digital component and for the day-to-day police work of first responders this distinction may no longer be relevant.[7]

Cyber-enabled crimes are those criminal acts that are committed by the use of ICT. The European Commission distinguishes between three types of cybercrime:

- Crimes specific to the internet, such as attacks against information systems or phishing (for example, fake bank websites to solicit passwords enabling access to victims' bank accounts).

- Online fraud and forgery – large-scale fraud can be committed online through instruments such as identity theft, phishing, spam and malicious code.

- Illegal online content, including child sexual abuse material, incitement to racial hatred, incitement to terrorist acts and glorification of violence, terrorism, racism and xenophobia (European Commission, 2019b).

Cyber-dependent crimes are traditional crimes that have greater impact and volume in the digital environment (for example, cryptomining and

[6] In this article internal security sphere personnel denotes all personnel working in the administrative area of the Ministry of the Interior, as well as cadets, students and staff of the Estonian Academy of Security Sciences.

[7] With the adoption of new technology, the boundaries between traditional crimes committed through ICT and so called pure cybercrimes have become blurred.

ransomware, attacks against critical infrastructure, and data breaches) (European Union Agency for Law Enforcement, 2018).[8]

The most common types of cyber-attacks are distribution of malware (especially ransomware), denial of service attacks, phishing, unauthorised access, intrusion by exploitation of vulnerability, fraud and abusive content (Europol, 2017). Also, data breaches have been growing exponentially in the last decade. This is a concern for law enforcement agencies who collect and transit large data bulks (for example, images, videos, geospatial intelligence, communication data, traffic data and data on financial transactions, etc.). The confidentiality, availability and integrity of data and ICT systems and networks must be protected not only against outsiders, but also against unintentional insider threats and technical mishaps.

The European Commission has recognised that criminals have greatly benefitted from technological development, but unfortunately measures for countering cybercrime are lagging behind (European Commission, 2019b). Moreover, this negative situation is exacerbated by a lack of cybersecurity specialists in Europe and North-America, as well as a low level of cybersecurity awareness in society as a whole. For example, by 2021 the lack of unfilled cybersecurity jobs will grow worldwide to 13,5 million (Cybersecurity Ventures, 2019a). By 2022 Europe will face an estimated skill gap of 350 000 cybersecurity professionals (European Union Institute of Security Studies, 2019). Estonia will need by 2023 up to 870 cybersecurity professionals more than it has today – which means that the current cybersecurity workforce should be increased by 86% (Melesk, 2019). In addition to the specialist cybersecurity workforce, cybersecurity competence of civil servants in public administrations must be enhanced, and the requisite study subjects must be included into the formal curriculum of public administration schools and universities at all three education levels (primary, secondary and tertiary).

[8] The Council of Europe's Convention on Cybercrime defines cybercrime based on four types of offences committed: offences against the confidentiality, integrity and availability of computer data and systems (illegal access, illegal interception, data interference and system interference); computer-related offences (computer-related forgery and computer-related fraud); content-related offences (offences related to child sexual abuse and exploitation); offences related to infringements of copyright and related rights (Council of Europe, 2001).

1.1 THE ESTONIAN EDUCATION SYSTEM, DIGITISATION AND CYBERSECURITY

According to Linnar Viik (2019), a recognised visionary who works as a programme director of the Estonian e-Governance Academy, in Estonia digital competence development has become a normal part of the education system. The same confidence cannot be expressed in regard to cybersecurity competence. The education system in the internal security sphere offers only one study programme at the master's level, which includes an elective cybersecurity and cybercrime course in scope of 3-6 academic credit points (EASS, 2019). There are no cybersecurity courses taught within the vocational and bachelors programmes.

In other Estonian vocational schools and universities technical cybersecurity-related courses have already been integrated in science, mathematics, engineering, technology (STEM) disciplines and in some public administration study programmes (for example, e-governance and technology policy programmes in TalTech). There are ICT-related non-technical courses available in the faculties of law and social sciences at Tartu University (for example, the information technology law and international relations study programmes). In some other faculties (humanities, medicine, earth sciences), however, no cybersecurity or ICT-related study courses have been included, even though the Estonian health care system is almost fully digitised (Melesk, 2019). Likewise, in the Estonian Defence Academy which provides formal education for the Estonian defence forces, cybersecurity subjects are currently present to a small extent in a few further specialisation areas such as communications.

1.2 CYBERSECURITY CHALLENGES OF THE ESTONIAN INTERNAL SECURITY SPHERE

In Estonia, internal security is considered part of a comprehensive defence principle, which consists in addition to upholding the internal security itself from other activities in four areas:

- Military defence
- Civilian support to military

- International action
- Government functioning, including the protection of essential services; and strategic communications (Government Office, 2017).

Cybersecurity is essential in ensuring the functioning of the government, society and economy as cyberspace permeates these four activity areas of a comprehensive defence approach. Whereas the Estonian Defence Forces have created advanced cyber capabilities such as cyber command, cyber range, and the Cyber Defence Unit of the Estonian Defence League, cybersecurity investments in the internal security sphere are lagging behind.

As a rule, law enforcement agencies in Europe are responsible for the prevention and response to cybercrime, curbing online disinformation and child abuse, as well as tracking and countering extremist activities in cyberspace. In Estonia, law enforcement is also responsible for issuing digital/electronic identity (e-ID) for citizens, residents and e-residents.[9] In the Estonian digital ecosystem a secure e-ID is a key component without which most of the essential services cannot be provided.

The Digital Agenda 2020 for Estonia includes the National Cybersecurity Strategy 2019-2022. The strategy assesses that in the next four years online criminal malevolence and economic loss resulting from it will further increase (Ministry of Economic Affairs and Communications, 2018a). A dramatic rise in cybercrime is predicated to cost $6 trillion annually worldwide, whereas costs from ransomware are predicted to exceed $20 billion by 2021 (Cybersecurity Ventures, 2019b). Globally the five most attacked industries are healthcare, manufacturing, financial services, government and transportation (Cybersecurity Ventures, 2019b). In Estonia, for example, tax, healthcare and financial services are almost exclusively digitised and thus especially vulnerable to cybercrime attacks. Since the early 2010s cybercrime has been growing in Estonia and the cost of cybercrime has doubled since the mid-2010s. For example, the number of digital fraud cases have doubled when compared to 2014. In 2017, malware, including ransomware attacks made up 70% of the registered cyber incidents (Ministry of the Interior, 2019).

[9] In Estonia e-ID is issued to all citizens and residents, as well as e-residents. It is based on an electronic identification document that can be an ID-card, SmartID, mobile-ID, digi-ID, or e-resident digi-ID. About 3000 e-services are provided by public administration authorities and about 2000 e-services by private sector companies. Almost all bank transactions are conducted online.

Essential services – in particular critical services such as financial systems, transportation, energy, telecommunications and healthcare – have become key targets of state and non-state cyber threat actors. Indeed, private cyber threat intelligent companies report that state-affiliated adversary groups regularly target critical services, especially the financial and energy sectors, as well as the defence industry and government. It has been disclosed that state threat actors have had an intention to cause physical damage to the equipment, which could cause longer power disruptions and physical harm to humans (Greenberg, 2019).

In addition to malicious cyber-attacks conducted by state-affiliated and cybercrime actors, technical failures and unknown vulnerabilities in the supply chain can cause interruptions in the provision of essential services. For example, in 2017 Czech computer scientists discovered a critical firmware vulnerability that affected almost 800 000 Estonian ID-cards and the government had to replace them (Information System Authority, 2017). This example illustrates how vulnerable the Estonian information society is on individual components of the digital ecosystem, which is made up of various digital infrastructures, web platforms, registers as well as third party suppliers and service providers, while the exact interdependencies between these components are difficult to determinate. This in turn complicates effective risk analysis and management. Thus, even if only one component fails the impact on the continuous operation of essential services and the functioning of the government, economy and society can be serious.

Indeed, in Estonia almost all essential services depend on ICT components almost totally. The majority of services are connected to the internet at least to an extent. As of today, there are almost 5000 electronic-services (e-services) accessible for users, whereas the majority of public services are digital and paper back-up copies are not provided (Härma, 2018). E-ID provides secure digital authentication and signature through which the end-user can use e-services such as declaring taxes, signing contracts, performing online banking transactions, accessing medical record, etc. The end-user can also encrypt documents and transmit and receive encrypted documents. Thus, e-ID is a central component of Estonia's digital ecosystem and as such it is designated in national regulations as a critical service that is subject to stronger cybersecurity risk management measures (Emergency Act, 2017).

There are four key stakeholders (three in the public sector and one in the private sector) who are responsible for e-ID management. It is essential that their requisite roles and responsibilities are clearly defined in regulations and well understood by all stakeholders, including law enforcement agencies. The Police and Border Guard Board that itself lacks technical capacity in E-ID development issues (digital and physical) identification documents. The Estonian Information System Authority, in the administrative area of the Ministry of Economic Affairs and Communications, is responsible for e-ID software development. The third stakeholder is a private company SK ID Solutions who provides trust service that enable the use of e-ID. The Ministry of Economic Affairs and Communications is moreover responsible for organising continuity of e-ID authentication and digital signature services (Emergency Act, 2017). The Ministry of the Interior together with other authorities in its administrative area (the Police and Border Guard Board, the Internal Security Service, and the Rescue Board) is responsible for three areas of internal security activity that pertain to ensuring safety in cyberspace:

- Crime prevention and criminal investigation (including cyber-enabled and cyber-dependent crime).
- Counterintelligence.
- Investigation of national security incidents.

Considering these responsibilities cybercrime knowledge and skills, as well as personal digital safety skills are essential competencies for first-responders. In the administrative area of the Ministry of the Internal Affairs dozens of specialist information systems and registers are used daily. For example, the e-police digital solution gives each police patrol car a real-time online connection to numerous national databases and the EU's Schengen information systems (e-Estonia, 2019). First-responders must be able to use national and international ICT systems and registers safely, including Estonian personal identification registers. Digital safety skills need to be trained from entry level jobs to senior leadership as a lack of these skills may cause sensitive and personal data leaks that can have serious national security implications.

Also, the application of disruptive technologies such as machine learning is actively pursued in the internal security sphere. For example, the Police and Border Guard Board uses a machine learning solution that

enables the location of police patrols to be predicted (Government Office, 2019). The Estonian government adopted in May 2019 a strategy, which in July 2019 was followed by an action plan, to accelerate AI implementation in the public and private sectors. As of today, 13 projects have been implemented in the public sector. The government will invest 10 million euros in the next three years (Government Office, 2019).

A study by the Estonian Academy of Security Science (2017) evinces that in the opinion of civil servants and the EASS cadets the latter's digital skills for using internal security information systems and databases are sufficient. However, the cadets are not confident in using the systems and cannot understand how data is created and transmitted between different databases, and what are the links and interdependencies between databases. This can lead to data corruption caused by human error, for example, if incorrect data is unintentionally inserted into one register that is replicated in or accessed from other registers. Moreover, the study determined that the cadets lack practical experience in using police information systems and registers (Estonian Academy of Security Science, 2017). Thus, even if the cadets believe their digital skills are sufficient, the lack of exposure to using police IT-systems and registers conceals the possible lack of digital safety skills. Most likely cadets' digital skills are better than their digital safety skills – a trend that is also prevalent in the general public. The study recommended that the EASS should give cadets a comprehensive view on interdependencies and links between police IT-systems and registers in a way that more general IT-knowledge will be linked to a work process (Ibid.). For example, the first-responder should understand how data is created and transmitted between the systems and how reliable it is.

In the area of data protection, EASS cadets had little knowledge about personal data protection regulations and encryption methods of data, as well as about processes and requirements for designating documents for official use (Ibid.). According to a recent opinion survey among the Estonian youth, 90% of young people use legacy digital authentication methods such as PIN codes instead of secure methods such as e-ID (Tarros, 2019). This illustrates that even though young people are considered digitally savvy, cybersecurity considerations tend to be an afterthought. In addition, the opinion survey identified that primary and secondary level education should give pupils more information about

Estonian e-services (Ibid.). This indicates that pupils and students alike would benefit from a better understanding of the Estonian digital ecosystem, including public and private sector e-services and e-solutions in order to enhance their digital skills and digital safety skills.

1.3 STRATEGIC GUIDELINES FOR COMPETENCE BUILDING IN THE ESTONIAN INTERNAL SECURITY SPHERE

The Estonian government has recognised that e-governance/e-state, the information society and e-services rely on strong cybersecurity, which is impossible to harness without an adequate number of quality specialised cybersecurity workers. The National Cybersecurity Strategy 2019-2022 sets out an objective of educating more technical cybersecurity experts. It also calls for developing cybersecurity competence across society, and all public servants (central government, municipal and local authorities) must possess a degree of cybersecurity competence (Ministry of Economic Affairs and Communications, 2018b).

The strategy highlights a need to provide cybersecurity formal education and in-service training for the defence forces and internal security workforce (Ministry of Economic Affairs and Communications, 2018b). The previous iteration of the strategy (National Cybersecurity Strategy 2014-2017) focused on cybercrime prevention in key activity areas. During that period, in July 2016 a new cybercrime prevention bureau at the Central Criminal Police of the Police and Border Guard Board was founded. During the present strategy period 2019-2022 the focus is on improving digital skills across the internal security workforce. In order to do so, cybersecurity study subjects need to be integrated into formal education and additional training provided to mid and senior level leadership.

In conjunction with these objectives set out in the National Cybersecurity Strategy 2019-2022, the Estonian government endorsed in September 2019 a Proposal for Updating the Internal Security Action Plan for 2020-2030. This strategic guideline recognises that the increasing number of

cyber-attacks and emerging technologies will have a negative impact on internal security. The guideline recommends that the forthcoming Internal Security Action Plan for 2020-2030 must design ends, ways and means to offer solutions to the following security challenges in the area of cybercrime and e-ID management:

- How to build capacity in the internal security sphere for responding to challenges stemming from the development of disruptive technology.
- How to establish capacity of situational awareness about cyber incidents in the area of internal security.
- How to improve capacity to remove illegal content from the internet.
- How to ensure adequate deterrence against cybercrime (Ministry of the Interior, 2019).

Given that these are the most important challenges for the internal security workforce, the following cybersecurity competences should be emphasized in formal education and additional training:

- Enhancing the understanding of the cybercrime phenomena and its current trends, as well as preventative and response measures (including digital evidence);
- Enhancing the understanding of regulations, procedures and technical tools in removing illegal online content.

In summary, in order to implement the strategic guidelines as set out in the National Cybersecurity Strategy, the Proposal for Internal Security Action Plan, and the EU policies, the EASS must introduce cybersecurity courses in all curriculums (vocational, bachelor, master's programmes). In addition, extra-curricular activities and additional training initiatives for mid and senior leadership and technical cybercrime investigators should be created.

1.4 CYBERSECURITY FORMAL EDUCATION IN THE ESTONIAN INTERNAL SECURITY SPHERE

The EASS provides vocational, bachelor and master's programmes for internal security employees (police officers, rescue service officers, prison officers, and tax and custom officers). As of September 2020, the EASS plans to integrate cybersecurity subjects into two programmes: the vocational curriculum "Police Service" and bachelor curriculum "Police Officer".

The majority of EASS graduates begin their professional careers at the Police and Border Guard Board in the following positions: border guard, patrolling police officer, traffic police officer, district police officer, youth police officer, and crime investigator. Whereas each of these positions has few unique duties, basic digital safety and cybersecurity skills for first-responders largely overlap. For example, youth police officers should have a good understanding of online privacy and security. Crime investigators should be competent in acquiring and handling digital evidence. Therefore, the basic competences that should be developed at EASS are related to e-ID management, cybercrime and data protection. As discussed earlier, every civil servant must have requisite knowledge about the Estonian digital ecosystem and its interdependencies (e-state, e-governance, e-services, etc.). Employees of internal security must understand what are the roles and responsibilities of different public and private actors in maintaining e-ID. In addition, the entry-level civil servants must be aware of the government strategic cybersecurity objectives and policies, cyber threats, and impact of disrupting technologies to cybersecurity. Everyone should receive requisite knowledge on digital evidence and challenges posed to crime investigation by the use of encryption applications (for example, WhatsApp, Signal, Telegram).

2. BEST PRACTICE FROM INTERNATIONAL ORGANISATIONS AND OTHER COUNTRIES

A. NATO

NATO and the Partnership for Peace (hereinafter NATO) cybersecurity reference curriculum for military officers and public servants provides an example of the cybersecurity topics that could be included into the curriculum of national defence and police academies for non-technical mid-level professionals (Costigan and Hennessy, 2016). The recommended teaching methods include interactive components (examining case studies, practical exercises and demonstrations). Four themes of the NATO curriculum are considered relevant to internal security employees:

- Cyberspace and the Fundamentals of Cybersecurity.
- Risk vectors.
- International cybersecurity organisations and standards.
- Cybersecurity management in the national context (Ibid.).

For example, cybersecurity management in the national context includes a sub-theme of digital forensics that covers methods and tools for analysing data acquired from computers, networks, mobile devices, databases and sensors. These competences are necessary for all internal security employees.

B. THE EU

In February 2019 Europol developed a *Cybercrime Training Competency Framework* targeting law enforcement personnel who deal with cybercrime, including first-responders. The framework includes required knowledge and skills at basic and expert levels across three dimensions: management, technical and investigation skills. The framework is recommended to be used by EU member states for defining education

and training requirements and the development of curricula (Sobusiak-Fischanaller and Vandermeer, 2019).

The EU has also created a *Cyber Competencies Career Path Matrix* in order to educate and train all military and civilian personnel who conduct Common Security and Defence Policy (CSDP) operations and missions. The training requirement analysis was conducted in 2019. The report of the training requirement analysis identifies tasks to be performed by civilian and military personnel, and respective competencies and skills required for performing them. It further identifies gaps in the existing training offer of the member states and EU education and training bodies, and proposes solutions to fill these gaps (including a list of new courses). The list of the suggested courses include the following areas of study: digital forensics, cybercrime investigation, and protection of critical infrastructure (European External Action Service, 2019).

Both documents (the framework and training requirement analysis) should be used by the EASS for developing cybersecurity curricula at a national level. The EU framework and analysis provides an overview of CSDP military and civilian personnel tasks and competencies (defined as knowledge, skills and abilities) that enable individuals to perform these roles as proficiently as possible. Similar assessment methodology could be used for developing competence frameworks and to design respective education and training courses at the national level.

C. THE UNITED STATES

The US has developed a nationwide NICE Cybersecurity Workforce Framework that "aims to codify cybersecurity talent; define the cybersecurity workforce in common terms; and tie the workforce's various jobs, competencies, and responsibilities into a common architecture (Paulsen, et.al. 2012). Organisations in the public and private sector can use the NICE framework as a reference source from which to develop training that meets their needs. However, the NICE framework is suitable for education, training, recruitment and retaining of the technical cybersecurity workforce, while the non-technical internal security workforce needs a more social science based curriculum. To fill this gap, Kessler

and Ramsay (2014) proposed a number of such cybersecurity courses. For example, a baseline course *Foundations of Information Security* targets all internal security students. The course includes a definition of information security, the need for this field of study, ethical and legal issues, risk management and planning, and information security technology (Ibid.).

D. FINLAND, GERMANY, THE NETHERLANDS, AND NORWAY

In Finland, Germany, the Netherlands, and Norway police academies teach basic cybersecurity and cybercrime knowledge at vocational and bachelor levels.

The Finnish Police University College (POLAMK) has integrated the secure use of IT and the use of a digital environment for crime investigation into bachelor and master's programmes (Toiviainen, 2019). POLAMK relies on cybercrime study materials of the European Cybercrime Training and Education Group, and cooperates in cybercrime advanced training with the European Union Agency for Law Enforcement Training (CEPOL) and the European Cybercrime Centre of EUROPOL (EC3). POLAMK runs several long-term education and training projects in the area of cybersecurity and cybercrime in cooperation with the Jyväsküla University of Applied Sciences. In 2018 a four-year €1.1 million project CYBERDI was initiated in the area of cybercrime prevention, awareness raising and capacity building in cooperation with the Jyväsküla University of Applied Sciences and several other domestic stakeholders (POLAMK, 2019a). A bachelor programme "Bachelor of Police Services" teaches cybersecurity and cybercrime themes as part of professional studies that provide the student with the vocational core competences required in policing. A course entitled "pre-trial investigation" includes the topics of cybersecurity environment, cybercrime, digital evidence, and the use of open source information and databases in police investigation (POLAMK, 2019b). POLAMK also provides education on open source intelligence (OSINT) as part of formal education and non-degree additional training. This type of training for employed

internal security professionals covers three themes: digital forensics, OSINT and tactical investigation methods (Toiviainen, 2019).

As part of elective studies an English language e-course "First Responders E-learning Course on Cybercrime" offered by the European Cybercrime Training and Education Group can be chosen. In this course a student learns about cybercrime, the internet, encryption, dark web and virtual currencies, and acquires skills to identify and seize potential digital evidence. The course includes topics such as open source intelligence, cyber-enabled and cyber-dependent crimes, seizure of digital evidence, and technical knowledge of software and technology (POLAMK, 2019c).

In Germany the Federal University of Applied Administrative Sciences has integrated cybercrime subjects at bachelor and master's levels. A bachelor programme "Criminal Police Officer at the Bundeskriminalamt" includes several ICT, cybersecurity and cybercrime subjects as part of a mandatory module that focuses on the gathering and use of information by the police and the cybercrime phenomena. The module consists of 240 study hours and accredits 8 ECTS credit points. The key subjects are basic principles of ICT, gathering and use of information, cybercrime and requisite police tasks and action in this field. It includes knowledge on the German legal framework in this field, for example, covert surveillance (Federal University of Applied Administrative Sciences, 2019a).

Also, a master's programme "Public Administration Police Management" includes a module on police information gathering (150 study hours and 5 ECTS credit points), which has ICT and cybercrime subjects. In addition, as part of the programme, master's students can choose an elective course about cybercrime (150 study hours and 5 ECTS credit points).

The Federal University of Applied Administrative Sciences offers a formal education diploma-programme "Police service in the Federal police (Diploma in Public Administration)," which includes a small amount of cybercrime related subjects (in total 24 study hours) such as international cooperation in cybercrime prevention, digital evidence and police tasks concerning online fraud (Federal University of Applied Administrative Sciences, 2019b).

The Dutch Police Academy, which provides formal education at vocational, bachelor and master's level, offers a two-year master's level programme - Criminal Investigator for police cybercrime investigators.

The Norwegian Police University College runs several advanced digital forensics e-courses in English for cyber investigators that are open to partners from other Nordic countries (Norwegian Police University College, 2019). Since 2014 it also runs an English language master's programme on digital forensics and cybercrime investigation.

In addition to incorporating the cybersecurity subject to compulsory courses in formal education, several police academies offer in cooperation with domestic and international partners additional advanced cybercrime training for cybercrime investigators.

3. BEST PRACTICE IN ESTONIAN SECONDARY AND TERTIARY FORMAL EDUCATION

There are several extra-curricular activities in primary and secondary schools starting from grade four to twelve.[10] For example, a digital competence pilot test was introduced in 2018 for 1400 pupils and a model for assessing pupils' digital competencies is available (Innove, 2018). The Information Technology Foundation for Education (HITSA) supports schools in developing digital competencies and digital safety of pupils and teachers, and offers a wide range of IT-related courses. Another example is the ProgeTiger progamme that includes courses on programming, 3D design, mechatronics, robotics, etc. In addition, HITSA offers a Safer Internet initiative for children, pupils, youth, teachers and parents with learning and teaching materials (HITSA, 2019). Currently there are some elective courses on cyber security in upper secondary level and the Põltsamaa municipal gymnasium has an elective cyber security course. The syllabus of the Põltsamaa municipal gymnasium could serve as a reference curriculum for integrating cybersecurity to the EASS curriculum.[11] Study materials include both technical and non-technical subjects about the information society and digital safety.[12] However, elective courses, student competitions and exercises in high schools are not coordinated, and access is random rather than systematic (Meleski, 2019).

In tertiary education the IT College of Tallinn University of Technology offers an English language Bachelor of Science programme "Cybersecurity Engineering". TalTech and the University of Tartu offer a joint Master of Science program "Cybersecurity", which includes digital forensics courses.

[10] For an overview of IT and cybersecurity education in Estonia see Lorenz, Kikkas, Sõmer, and Laugasson, 2019.

[11] The syllabus is available at https://onedrive.live.com/view.aspx?resid=7B5915FDC0CD4BE4!9609&ithint=file%2cdocx&authkey=!AGo9f4nh7CguAjI

[12] The syllabus is available at https://drive.google.com/drive/folders/0B431U6eEm9oVY081WEhMaENQSFk

The University of Tartu has also integrated cybersecurity subjects to several non-technical programmes, for example, an elective course in the Master of Arts programme "International Law and Human Rights." Likewise, in the Faculty of Social Sciences programmes, cybersecurity is designated as one of the study objectives; however, at the Faculty of Arts and Humanities, the Faculty of Medicine and in Earth Sciences, cybersecurity-related study subjects have not been introduced (Praxis, 2019).

The TalTech master's programme "Law of Technology" has elective courses for cyber defence and law, e-governance, digital evidence and e-state IT solutions. Mandatory cyberspace-related subjects are regulations pertaining to the protection of ICT infrastructure, human rights, ethics and technology, as well as law on intellectual property. In addition, a master's programme "European Union and International Law" includes courses on cyber defence and law, legal aspects of e-governance, and the rights of internet users.

The TalTech master's programme "Technology Governance and Digital Transformation" focuses on various IT-subjects, and has an elective course on the fundamentals of information security. The "International Relations and European-Asian Studies" master's programme includes an elective course on cybersecurity, and the Faculty of Economics master's programmes include technology courses such as big data and registers. Also, the public sector leadership and innovation master's programme includes technology, big data, e-governance, and e-democracy courses. The TalTech master's programme on International Relations and European Studies, as well as the EASS master programme on Internal Security include an elective cybersecurity course.

Finally, TalTech has launched it's "TalTechDigital" initiative with an e-course "DigiWisdom" covering basic digital safety skills, which was piloted for academic and administrative staff in 2018 (Lorenz, Kikkas, Sõmer, and Laugasson, 2019).

3.1 BEST PRACTICE OF THE MINISTRY OF DEFENCE AND THE NATIONAL DEFENCE ACADEMY

The National Defence Academy does not provide cybersecurity courses as part of a master's programme. Both vocational and bachelor programmes contain few ICT-related subjects in only one specialisation area of the curricula (communications). For example, as part of specialisation in communications, the curricula of a vocational programme "Military leadership for Senior Non-commissioned Officers" includes subjects such as IT and cybersecurity foundations, and methods to ensure cybersecurity. Also, bachelor programmes provide to those students who specialise in communications tactical level knowledge on ICT and cybersecurity foundations. The bachelor programme also includes themes of cyber hygiene and cyber threats. However, those students who choose other areas of specialisation do not currently receive any cybersecurity education (The National Defence Academy, 2019).

The Ministry of Defence has launched a Cyber Olympic programme for young talent. It includes a CyberCracker competitions for two age groups at primary and secondary education level and a CyberSpike competition at secondary and tertiary level for ages 14-24 (Taltech, 2019a). Estonian youth teams participate at the annual European Cybersecurity Challenge competition.

Since 2015 the Ministry of Defence also supports a 35-hour advanced cybersecurity course in a Põltsamaa municipal gymnasium, as well as the integration of cybersecurity into national defence courses in gymnasiums and vocational schools. The national defence course gives an overview of cyber defence in the military, and a study book published by the Ministry of Defence includes a chapter on cybersecurity (Kaas, 2019).

As part of compulsory military service for male citizens (in Estonia, conscription is voluntary for females) a pilot cyber conscription programme was launched in 2016. There are plans to extend the current eleven-month duration of the cyber conscription service to twelve months (Err, 2018). Sõmer, Ottis, and Lorenz (2019) have suggested that cyber training of the conscription service should include subjects relevant

for cybercrime investigators (digital forensics, open source and signal intelligence). According to these scholars, conscripts could receive a certificate of training after completion of service. They propose that such on-the-job training could be transferred to academic credit points or diplomas at IT and cybersecurity programmes in universities and vocational schools (Ibid.). Against this background, if cyber conscription will provide know-how on digital forensics and digital evidence, as well as open source and signal intelligence, the conscription service could be used as a recruitment base for cybercrime investigators of the Central Criminal Police.

The Cyber Defence Unit of the Estonian Defence League is a public-private and civil-military cooperation model that pools cybersecurity talent and skills from the public and private sector in order to support national level cybersecurity. The unit can be assigned a task of assisting public and private sector companies in protecting essential services, as well as municipal and local authorities where the level of cybersecurity tends to be lower. The members come from diverse technical and non-technical (legal, policy, academic, etc.) backgrounds and contribute voluntarily without receiving any pay. The members of the unit assist upper secondary schools in introducing cybersecurity subjects to pupils (Sõmer, Lorenz, Kikkas, and Laugasson, 2019).

The Ministry of Defence in cooperation with other domestic partners supports an annual high-level e-state and cybersecurity course. The training audience includes top opinion leaders as well as mid and senior level leadership from the media, business, public administration, civil society, and other areas of societal and economic activity. It is a non-technical course that presents views of senior experts about technology, cyber threats, cybercrime, adversary activity, legal and strategic communication issues, as well as strategies, policies and measures of cybersecurity in NATO, the EU and Estonia.

4. DISCUSSION AND POLICY RECOMMENDATIONS

The article revealed that enhancing general cybersecurity and cybercrime competence of internal security public servants is an important objective of the Estonian government. Many countries in Europe and beyond struggle with finding enough resources to support cybersecurity education and training, as well as cybersecurity workforce development. In order to enhance cybersecurity competences of internal security employees the government of Estonia and the Ministry of the Interior should allocate substantial funding to support the EASS initiatives. The ends, ways and means for doing so should be determined with the Internal Security Action Plan 2020-2030. The EASS should pursue cooperation and partnerships with national and international partners for greater synergy and cost efficiency in developing programmes for specific training audiences.

In summary, this article discussed cybersecurity and cybercrime education and training efforts of foreign police universities, the NATO reference curricula and syllabus of Põltsamaa municipal gymnasium. Based on the comparative analysis, a number of common themes across countries was identified. It is suggested that the same themes should be integrated into the EASS programmes given they are adapted to the context of an Estonian digital ecosystem. In addition, the EASS curricula should address in depth those digital safety and cybersecurity issues that pertain to tasks of first-responders. For example, e-ID and data protection are subjects that pertain directly to first-responders on-job responsibilities and tasks, and the previous research and expert opinion indicates that the knowledge on these issues among police cadets and employed first-responders is insufficient.

Therefore, future first-responder job descriptions should include requirements for skills required for the secure use of internet and information systems, as well as about more general cybersecurity and cybercrime knowledge. In addition, the EASS curriculum should provide knowledge and practical experience to students about the secure and safe use of police information systems and state registers, in particular about

data protection regulations and methods. As the previous research has shown the EASS students do not understand how data is created and transmitted in and between different information systems and what are the implications for data protection.

Lastly, the impact of new courses and study subjects, as well as appropriate teaching methods and tolls should be periodically assessed (and amended as needed), and student and teachers feedback collected. The content and teaching methods and tools should be updated regularly so that they correspond to real life problems that professionals at the Police and Border Guard Board encounter, and that teachers are using the same software and IT systems that are used by employed professionals.

Given that the National Defence Academy has integrated to date only a few subjects about cybersecurity fundamentals and cyber defence in the Estonian Defence Forces to its own curricula, it could cooperate with the EASS and HITSA to develop a joint cybersecurity curriculum and attractive digital study materials.

For example, HITSA has made available e-textbooks and study videos for primary and secondary school pupils and teachers. Interactive video games could be developed for defence and police cadets. Teachers for technical subjects should be recruited from technical universities (IT college, TalTech, etc.) and among cybercrime prevention professionals working at the Police and Border Guard Board, whereas general knowledge subjects could be taught by the Cyber Defence Unit of the National Defence League.

In the longer-term cybersecurity courses should be integrated into all programmes of the EASS, including the rescue service, correction and prison officials, and customs and tax officials. A cyber hygiene e-learning course developed by an Estonian company is employed in many government authorities and Estonian universities. The e-course is mandatory for public servants of the Police and Border Guard Board. The Estonian Information System Authority likewise uses this tool to improve cyber hygiene of public servants and family physicians. It is recommended the e-course should be compulsory for EASS teaching personnel, administrative staff, and police and border guard cadets in order to improve

their cyber hygiene skills.[13] The EASS could cooperate with other domestic partners, such as the Cyber Defence Unit of the Estonian Defence League to provide non-formal activities such as student camps, competitions, and hackathons to the cadets. The Cyber Defence Unit could also regularly brief EASS students and staff on how to improve cyber hygiene.

As part of elective studies EASS students should be able to choose advanced ICT and cybercrime investigation courses provided by other universities (TalTech, IT college) and through the Erasmus student exchange in the police academies of Nordic countries. Advanced level cybercrime training for cybercrime investigators (cyber criminalists) should be conducted in cooperation with technical universities and other educational institutions. International cooperation with Nordic countries and European partners could offer study opportunities with minimal costs (for example, the Norwegian offers digital forensics e-courses in English).

First-responders working at the Police and Border Guard Board should pass the e-course for first responders provided by the European Cybercrime Training and Education Group.[14] In addition, a new e-learning course that targets all law enforcement officers, prosecutors and judges who deal with cybercrime, including first responders is under development. The course includes topics such as identifying, preventing and investigating cybercrime, conducting first response, the legal framework, etc.[15]

All first-responders must have a profound understanding of judicial and security implications of the inappropriate use of e-ID in Estonia. For example, people may not fully acknowledge that by entering PIN codes digitally they will be subject to legally binding obligations because a digital signature is equivalent to a hand-written signature. Likewise, there have been fraud cases where the elderly may not fully comprehend the reasons why sharing their ID-card and PIN codes with third persons is equivalent to transferring their digital identity. In case of doing so for

[13] Description of the course is available at the company website https://cybexer.com/cyber-hygiene-e-learning-course/.

[14] The course description is available at https://www.ecteg.eu/running/first-responders/.

[15] The draft version as of October 2019 of the course description is available through national representatives.

internet voting will violate a principle of secrecy and in their case result in unwanted financial obligations. Therefore, first-responders should be able to explain to less tech-savvy e-ID users the legal framework and reasons why digital identity is only for personal use. First-responders should also have an understanding on how to protect personal data in police registers, how the data is created and how it is used for the identification of persons of interest (Kirch, 2019). Both of these aspects are specific to the Estonian digital infrastructure, thus if a foreign reference curriculum will be used it should be complemented by basic knowledge about the Estonian system. There is a need to provide basic cyber security skills for all cadets and focus on more specialised training for cybercrime investigators.

In addition to students, cyber security and digital competences need to be part of teacher training. HITSA could provide basic and additional training for teachers, involving cyber security experts, trainers in companies, public sector and potentially also talented students, as well as support the development of a support network for teachers, education technologists and science schools for more interested students (Melesk, 2019).

Students who will complete the cyber conscription service in the Estonian Defence Forces and who do not wish to work for the military could be encouraged to study at the EASS and join the cybercrime investigation team at the Central Criminal Police after completion of their studies. The cyber conscription training prepares conscripts not only in defending military networks, but also provides skills on gathering digital evidence as part of digital forensics, OSINT and signal intelligence. Those conscripts who do not start working as active duty military should be encouraged to join law enforcement. As proposed earlier in this article, extra-curricular cybersecurity activities for EASS students should be initiated in order to find and develop cybersecurity talent for the law enforcement workforce and existing programmes (competitions, summer camps) should be extended to the internal security sphere.

The extra-curricular cybersecurity training initiatives of the Ministry of Defence should be further analysed with a view to extend benefits to the internal security sphere by creating joint projects. The EASS should initiate similar extra-curricular activities (student competitions and

exercises) and cooperate with the Ministry of the Defence in finding synergy between each other's extra-curricular programmes and initiatives.

The Ministry of the Interior proposed in September 2019 the creation of a 700-person armed internal security reserve force that would be deployed in the case of a public order crisis. According to him the force can be deployed in internal security scenarios such as mass riots and evacuations, protection of state borders and of objects of essential services. The cost for training and equipment are estimated about 20 million euros during the next four years, and it would be composed of graduates of the EASS, former police officers and members of military reserve who have competed their conscription service, including military police training (Tooming, 2019). In order to support a response to a cyber emergency and day-to-day protection of cyberspace a voluntary civilian cyber team could be created composed of students, staff and alumni of the EASS as well as professionals from the internal security sphere. Previous research shows that cyber security skills are mainly acquired outside of formal education, through hobby groups or self-learning and these possibilities should be created for the cadets of EASS.[16] The main objectives of a voluntary cyber team could be twofold:

- Supporting cybersecurity in the internal security sector by raising awareness and conducting training.

- Supporting the response to a cyber emergency.

For example, in October 2019 the EASS organised a non-technical hackathon where teams of EASS students were tasked to come up with innovative ideas on how to apply simulation, virtual reality and other high-tech tools in to the study process. Such competitions, camps and other activities could be organised by a voluntary cyber team in order to raise cybersecurity awareness and interest in ICT and cybersecurity among students, staff and professionals. The team could participate in national and international cybersecurity competitions (for example, Garage48 Cybersecurity Hackathon organised by the University of Tartu), and organise training events (summer camps, competitions) for EASS students and staff.

[16] For example, see Sõmer T., et. al., 2019.

In case of a serious cyber-attack or incident that has national security implications, members of the team could support response activities of internal security authorities, the government Computer Emergency Response Team of the Estonian Information System Authority, and the Cyber Defence Unit of the Estonian Defence League. During an armed conflict the team would not become a part of the wartime structure of the Estonian Defence League. A civilian voluntary organisation may attract additional members including women who may not consider the military nature of the Cyber Defence Unit appealing. The organisation can serve as a focal point to establish and maintain joint projects with the industry, such as Estonian companies developing AI and cybersecurity solutions. Stronger cooperation with the industry is necessary to implement AI and digitisation solutions to analyse large datasets such as drone and satellite data.

Based on the research presented in this article the author recommends the EASS to integrate in the vocational and bachelor level programmes the following main themes from autumn 2020:

- Introduction to and fundamentals of cybersecurity and cyber threats.
- The impact of disruptive technologies on cybercrime, government and law enforcement.
- Introduction to cybercrime.
- National and EU regulations in cybersecurity and data protection as well as international regulations (for example, the Budapest convention).
- Key international organisations pertaining to cybercrime prevention and response.
- Principles and foundations of secure e-government and digital infrastructure (e-ID, e-services, etc.) in Estonia.
- Cybercrime prevention, response and investigation, including gathering and handling of digital evidence.
- The use of ICT for police investigations and gathering information.
- National and international cooperation in cybercrime prevention.

These subjects can be divided to several courses, and the descriptions of courses must include the purpose of the course, learning objectives, competences and qualifications acquired by students. Study methods

should include classroom and individual study, group and individual assignments, written papers and presentations, a list of mandatory readings, interactive workshops, demonstrations, and practical exercises. New learning paradigms and attractive learning materials (demonstrations, simulations, computer-game-based learning), digital materials (videos, e-courses, -tests, -books, etc.) and cybercrime incident analysis computer software programmes should be used. Cybersecurity and cybercrime study subjects could be integrated into the existing modules first as pilot courses, and after collecting students and teachers feedback the content could be reviewed and updated regularly.

It should be noted that the findings within this article are subject to a number of limitations. It is not possible to assess the impact of teaching cybersecurity study subjects to the actual competences of first responders employed in law enforcement agencies. Introduction of cybersecurity subjects into the curriculum of police academies has been a recent initiative in most countries and assessing the impact of these models to improve job-related tasks can be performed after the graduates of these courses have started their professional careers. Cybersecurity education and training is a rapidly evolving discipline and all curricula should be reviewed and updated regularly. The scope of this study dictates that this is not a full or comprehensive review of the existing best practices, and does not examine the application of the cybersecurity workforce building frameworks in the Estonian context. The article provides an overview of current cybersecurity education initiatives in Estonia, and in some other countries, as well as the EU and NATO. The article does not capture the full perspectives of all subject matter experts in the field, but the author reviewed relevant documents and conducted interviews to produce a review of cybersecurity education in the Estonian internal security sector. In the course of future research the proposed study themes should be specified at two or four levels of proficiency (basic and advanced or basic, intermediate, advanced and expert).

CONCLUSION

The article described strategic guidelines of the Estonian government for cybersecurity competence building in the internal security sphere. It gave an overview of the existing cybersecurity education in Estonia and of cybersecurity formal education in police universities in Finland, Germany, the Netherlands and Norway.

The current deficit of digital skills, shortness of cybersecurity and cybercrime knowledge, skills and abilities of the internal security personnel are risks to national security and public order. Currently EASS students do not have a clear understanding of the Estonian digital ecosystem and interdependencies of its components, and enough knowledge about data protection principles, regulations, and measures. There is also no training provided to improve digital safety skills such as an e-learning course and test. The author recommended study subjects to be included as a pilot project to the EASS curriculum from the autumn semester of 2020. A closer cooperation with the Ministry of Defence, which has initiated and supports a number of initiatives for cybersecurity competence building through extra-curriculum activities, is also recommended.

Contact:

Piret Pernik
E-mail: piretpernik@icloud.com

REFERENCES AND SOURCES

Costigan S. S. and Hennessy, M. A. eds. (2016) *Cybersecurity. A Generic Reference Curriculum.* [Online source] Available from: https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2016_10/1610-cybersecurity-curriculum.pdf.

Council of Europe. (2001) Budapest Convention: Convention on Cybercrime, Budapest, 23 November 2001. [Online source] Available from: https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081561.

Craglia M. (Ed.), Annoni A., Benczur P., Bertoldi P., Delipetrev P., De Prato G., Feijoo C.,

Fernandez Macias E., Gomez E., Iglesias M., Junklewitz H., López Cobo M., Martens B., Nascimento S., Nativi S., Polvora A., Sanchez I., Tolan S., Tuomi I., Vesnic Alujevic L. 2018. Artificial Intelligence - A European Perspective, EUR 29425 EN, Publications Office, Luxembourg, 2018, ISBN 978-92-79-97217-1, doi:10.2760/11251, JRC113826.

Cybersecurity Ventures. (2019a) Cybersecurity Almanac: 100 Facts, Figures, Predictions and Statistics. [Online source] Available from: https://cybersecurityventures.com/cybersecurity-almanac-2019/.

Cybersecurity Ventures. (2019b) Cybercrime Damages $6 Trillion By 2021. [Online source] Available from:

https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/.

EASS [Estonian Academy of Security Science]. (2017) *Information Systems Training of Cadets of the Police and Rescue College of the Estonian Academy of Security Science*.

EASS [Estonian Academy of Security Science]. (2019) *Internal Security Master Programme. Curriculum.* [Online source] Available from: https://www.sisekaitse.ee/sites/default/files/inline-files/Sisejulgeoleku%20magistri%20%C3%B5ppekava_0.pdf.

e-Estonia. (2019) *Security and Safety, e-Police*. [Online source] Available from: https://e-estonia.com/solutions/security-and-safety/e-police/.

Emergency Act. (2017) *State Gazette.* [Online source] Available from: https://www.riigiteataja.ee/en/eli/525062018014/consolide.

European Union Agency for Law Enforcement Cooperation. (2018) *Internet Organised Crime Threat Assessment*. Available from: European Union Agency for Law Enforcement Cooperation 2018.

European Union Institute of Security Studies. (2019) *EUISS Yearbook of European Security.*

[Online source] Available from: https://www.iss.europa.eu/sites/default/files/EUISSFiles/YES_2018.pdf.

Err. (2018) *New EDF commander favours extending conscription for some fields*. 6 December 2018. [Online source] Available from: https://news.err.ee/882577/new-edf-commander-favours-extending-conscription-for-some-fields.

European Commission. (2019a) *Horizon 2020. Programme 2018-2020.* [Online source] Available from: https://ec.europa.eu/research/participants/data/ref/h2020/wp/2018-2020/main/h2020-wp1820-security_en.pdf.

European Commission. (2019b) *Cybercrime*. Migration and Home Affairs. [Online source] Available from: https://ec.europa.eu/home-affairs/what-we-do/policies/organized-crime-and-human-trafficking/cybercrime_en.

Europol. (2017) *Common Taxonomy for Law Enforcement and CSIRTs.* Europol EC3 European Cybercrime Centre. Version 1.3. [Online source] Available from: https://www.europol.europa.eu/publications-documents/common-taxonomy-for-law-enforcement-and-csirts.

Federal University of Applied Administrative Sciences. (2019a) *Criminal Police Officer at the Bundeskriminalamt.* Module 10.

Federal University of Applied Administrative Sciences. (2019b) *Police Service in the Federal Police (Diploma in Public Administration).*

Government Office. (2017) *National Defence Development Plan 2017-2026.* [Online source] Available from: https://www.valitsus.ee/sites/default/files/content-editors/arengukavad/rkak_2017_2026_avalik_osa.pdf.

Government Office. (2019) *AI Implementation Report of Estonia* [Eesti tehisintellekti kasutuselevõtu aruanne]. [Online source] Available from: https://www.riigikantselei.ee/sites/default/files/riigikantselei/strateegiaburoo/eesti_tehisintellekti_kasutuselevotu_eksperdiruhma_aruanne.pdf.

Greenberg, A. (2019) New Clues Show How Russia's Grid Hackers Aimed for Physical Destruction. *Wired*. [Online source] Available from:

https://www.wired.com/story/russia-ukraine-cyberattack-power-grid-blackout-destruction/).

Information System Authority. (2017) *ROCA Vulnerability and eID: Lessons Learned*. [Online source] Available from: https://www.ria.ee/sites/default/files/content-editors/kuberturve/roca-vulnerability-and-eid-lessons-learned.pdf.

Innove. (2019) Täna algab pilootprojekt, mis annab esimest korda võimaluse mõõta õpilaste digioskusi. [Online source] Available from: https://www.innove.ee/uudis/tana-algav-tasemetoo-annab-esimest-korda-voimaluse-moota-opilaste-digioskusi/.

International Telecommunication Union. (2018). The Global Cybersecurity Index 2018. Available from: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf.

HITSA [The Information Technology Foundation for Education]. (2019) ProgeTiigri koolitused. [Online source] Available from: https://www.hitsa.ee/ikt-hariduses/koolitused/progetiigri-koolitused.

Härma, K. (2018) Kuu pärast tuleb olla e-teenustega valmis uueks ID-kaardiks. Äripäev. [Online source] Available from: https://www.aripaev.ee/uudised/2018/11/08/kuu-parast-tuleb-olla-e-teenustega-valmis-uueks-id-kaardiks.

Kaas, K. (2019) *Riigikaitseõpik gümnaaasiumitele ja kutseõppeasutusele*. Ministry of Defence. Avita publishing, Tallinn. [Online source] Available from:

https://drive.google.com/file/d/1cY6MzkbJeFmZ3-60XHoESXH5h7ZPkkLY/view.

Kessler G., and Ramsay J. (2014) *A Proposed Curriculum in Cybersecurity Education Targeting Homeland Security Students.* 47th Hawaii International Conference on System Sciences, 2014. DOI: 10.1109/HICSS.2014.605.

Kirkpatrick D., Hubbard, B. (2019) Attack on Saudi Oil Facilities Tests U.S. Guarantee to Defend Gulf. *The New York Times.* 19 September 2019. [Online source] Available from: https://www.nytimes.com/2019/09/19/world/middleeast/saudi-iran-attack-oil.html.

Kirch, K. (2019) Email communication with the author. September, Tallinn.

McAfee (2018) 2019 Threats Predictions. [Online source] Available from: https://securingtomorrow.mcafee.com/other-blogs/mcafee-labs/mcafee-labs-2019-threats-predictions/.

Melesk K., Mägi E., Koppel K., Michelson A. (2019) *Labor force and skills need in cyber security.* Praxis. [Online source] Available from: http://www.praxis.ee/wp-content/uploads/2018/04/K%C3%BCberturbe-uuring_aruanne-23_04_2019.pdf

Ministry of the Interior. (2019) *The Internal Security Action Plan 2020-2030* [Siseturvalisuse arengukava 2020-2030].

Ministry of Economic Affairs and Communications. (2018a) *Digital Agenda 2020 for Estonia. Updated 2018.* [Online source] Available from: https://www.mkm.ee/sites/default/files/digital_agenda_2020_estonia_engf.pdf.

Ministry of Economic Affairs and Communications. (2018b) *National Cybersecurity Strategy 2019-2022.* [Online source] Available from: https://www.mkm.ee/sites/default/files/kyberturvalisuse_strateegia_2022_eng.pdf.

National Defence Academy. (2019) *Military Leadership for Land Force. Curriculum.* [Online source] Available from: https://www.kvak.ee/

files/2019/05/S%C3%B5jav%C3%A4eline-juhtimine-maav%C3%A4es-rakendusk%C3%B5rgharidus%C3%B5pe.pdf.

Norwegian Police University College. (2019) *Studies in English.* [Online source] Available from: https://www.phs.no/en/studies/post-graduate-studies/.

Paulsen, C., Newhouse W., McDuffie, E., Toth, P. (2012) NICE: Creating a Cybersecurity Workforce and Aware Public. IEEE Security and Privacy. May-June 2012, pp. 76-79, vol. 10. DOI: 10.1109/MSP.2012.73.

POLAMK [The Finnish Police University College]. (2019a) *CYBERDI.* [Online source] Available from: https://jyvsectec.fi/2018/10/cyberdi/.

POLAMK [The Finnish Police University College]. (2019b) *Bachelor of Police Services. Curriculum 2018-2020.* [Online source] Available from: https://www.polamk.fi/instancedata/prime_product_julkaisu/intermin/embeds/polamkwwwstructure/61434_Curriculum_Bachelor.pdf?1180e46df085d688).

POLAMK [The Finnish Police University College]. (2019c) *Poliisi (AMK) -tutkinto Vapaasti valittavat opintojaksot, jotka eivät ole opetussuunnitelmassa Lukuvuosi 2018 – 2020.* [Online source] Available from: https://www.polamk.fi/instancedata/prime_product_julkaisu/intermin/embeds/polamkwwwstructure/84011_Poliisi_AMK_opsin_ulkopuoliset_vapaasti_valittavat_opintojaksot_2019_2020.pdf?c5ec6b44fa31d788).

Silberglitt R., Chow B., Hollywood J., Woods, D., Zaydman M., Jackson B. (2019), Visions of Law Enforcement Technology in the Period 2024-2034

Report of the Law Enforcement Futuring Workshop, Rand Corporation. [Online source] Available from: https://www.rand.org/pubs/research_reports/RR908.html.

Sobusiak-Fischanaller M., and Vandermeer Y., (2019) *Cybercrime Training Governance Model. Cybercrime Training Competency Framework.* European Cybercrime Training and Education Group. [Online source] Available from: https://rm.coe.int/3148-2-3-ecteg-16-cy-train-module/1680727f34.

Skattor, B. (2019) Trust & Security: building trust for use of AI by law enforcement. [Presentation] Tallinn Digital Summit 2019, Tallinn, 16 September 2019.

Sõmer T., Ottis R, Lorenz B. (2019) *Developing Military Cyber Workforce in a Conscript Armed Forces: Recruitment, Challenges, and Options.* ICCWS 2019: International Conference on Cyber Warfare and Security. 28 February - 1 March, South Africa.

Sõmer T., Lorenz B., Kikkas K., and Laugasson A. (2019) *Cybersecurity within the Curricula of Informatics: The Estonian Perspective.* 12th International Conference on Informatics in Schools (ISSEP 2019). 18-19 November 2019,

Larnaca. To be published in Lecture Notes on Computer Science conference proceedings.

TalTech. (2019a) *About the project.* [Online source] Available from: https://sites.google.com/view/kyberolympia/eng/about-the-project.

Tarros, M. (2019) [Presentation] *Digital Agenda For Estonia 2021+.* Tallinn, 16 September 2019.

Toiviainen, T. (2019) Interview with the author. April, Tampere.

Tooming, M. (2019) Sisekaitse reservi loomine nõuab nelja aastaga 20 miljonit eurot. *Err.* [Online source] Available from: https://www.err.ee/981248/sisekaitse-reservi-loomine-nouab-nelja-aastaga-20-miljonit-eurot.

Viik, L. (2019) *Exclusive overview of the story of e-Estonia and will zoom into the future plans to push e-Estonia even further into the future.* [Discussion] Digital Agenda For Estonia 2021+, Tallinn, 16 September 2019.

Wright, N. (2018) *AI, China, Russia, and the Global Order: Technological, Political, Global, and Creative Perspectives. A Strategic Multilayer Assessment (SMA) Periodic Publication.* Department of Defense, Joint Chiefs of Staff. December 2018, pp. 1-2. [Online source] Available from: https://nsiteam.com/social/wp-content/uploads/2018/12/AI-China-Russia-Global-WP_FINAL.pdf.

WORK, PREY, LOVE: A CRITICAL ANALYSIS OF ESTONIAN CYBERCRIME CASE LAW 2014-2019

Kristjan Kikerpill, MA
Independent researcher

Keywords: Cybercrime, Case law, Qualitative content analysis, Convention on Cybercrime, Directive 2013/40/EU

ABSTRACT

The current study takes a closer look at the people behind the 'cybercrime' moniker in Estonia. Following a socio-legal research approach, qualitative content analysis and systematic legal interpretation were used to analyse N=42 Estonian court judgements and decisions delivered between 01.01.2014 and 10.08.2019. The results show relative uniformity in crimes involving multiple perpetrators, where the primary distinguishing factor was the level of technical sophistication of the crimes. Crimes committed by individual perpetrators exhibited more variation, ranging from low-tech account takeovers perpetrated by broken-hearted ex-partners to active use of malware and signals jamming. The systematic legal analysis showed that the current system of cybercrime provisions in the Estonian Penal Code is unnecessarily scattered, because the substantive differences between the provisions are insignificant and do not adequately reflect the inherent characteristics of cybercrime. The article thus calls into question whether the legislator has taken the easy road by mechanically adopting international instruments (Council of Europe's Convention on Cybercrime and Directive 2013/40/EU) into domestic criminal law.

INTRODUCTION

Report after report states that cybercrime is growing and diversifying, with account takeovers and various types of fraud still dominating (LexisNexis, 2019). Criminals can even hold entire townships to ransom (Newman 2018; Torbet 2019; Gallagher 2019). However, most crime never crosses the news threshold (Felson and Boba, 2010, pp. 1-4). While cyber-attacks that entail far-reaching consequences to already worried populations have become an inconvenient social reality (European Commission, 2017, p. 7), they are still in the minority compared to run-of-the-mill criminal offences such as fraud (McGuire, 2018). Conventional crime statistics can provide some insights to the general state of affairs, but are rarely entirely reliable in terms of crime-related social reality because the numbers suffer from chronic underreporting (UNODC 2013). In the past decade, criminological research into phishing (Hutchings and Hayes, 2009; Atkins and Huang, 2013; Leukfeldt, 2014), cybercrime criminal groups (Soudjin and Zegers, 2012; Leukfeldt and Jansen, 2015), identity theft (Reyns, 2013) as well as malware victimisation (Bossler and Holt, 2009; Leukfeldt and Yar, 2016) has significantly improved our knowledge about the nature of such crimes and the modus operandi of perpetrators. However, criminological research often analyses 'crime' as merely a generic social phenomenon in a way that does not inform how relevant law functions or would function in various cybercriminal situations. Additionally, only addressing crime from a doctrinal legal research perspective leaves social reality on the side-lines.

Doctrinal legal research primarily uses description and interpretation as its methods whereas little, if any, attention is given to sample formation (van Hoecke, 2011, pp. 1-18). The lack of attention to sample formation is precisely why legal opinions that only employ supportive examples in their line of argumentation run the risk of involving extreme personal (i.e. author) bias on legal matters. Another major limitation of this approach is its inclination towards creating an overly dramatic public perception of criminal events by focussing on high-profile cases (Wall, 2008; Felson and Boba, 2010). Hence, to address and counteract the inherent value-based bias of doctrinal legal research as well as to analyse cybercrime as a specific law-based phenomenon rather than generic social malice, the

current article adopts a socio-legal approach for the study of cybercrime, which is a more recent addition to the body of knowledge (Dizon, 2016; Kikerpill and Siibak, 2019).

To gain an improved understanding about the real people and the real crimes behind the 'cybercrime' moniker from the perspective of applicable criminal law, it is paramount to investigate the one place where social and legal reality always meet - the courtroom, and the resulting case law. Analysis of court and law enforcement documents is common in criminological research (Leukfeldt, 2014; Lavorgna, 2015), but is mostly only used to glean insights about the activities. Therefore, the research design of the current article offers new insights by providing a criminal-law-in-action perspective that analyses both the social and legal reality of cybercrime. Furthermore, exploring the actions of cybercriminals operating in Estonia, which has often been referred to as the most wired country in the world (Reynolds 2016, Heller 2017), would add an interesting layer to the analysis. For example, analysing the case law from Estonia enables me to investigate whether punishable offences in Estonia are committed by innovative technology savants or common people who, among other methods, use computers to commit acts and create consequences that are unpleasant and deemed socially and legally unacceptable. To achieve these goals, the current research takes a closer look at the perpetrators of cybercrimes, their actions as well as the contexts within which such actions were committed as recorded in the indictments and arguments available in Estonian cybercrime case law from 2014-2019.

The article at hand begins by providing a brief overview of the history of cybercrime provisions in Estonian criminal law as well as the methods used in collecting and analysing relevant case law are described in more detail. The third section presents the findings and qualitative analysis, focussing on offences resulting from romantic/personal relationships, including employment-related matters, and predatory crimes. Based on the findings and qualitative analysis, the final section provides a systematic legal interpretation of the chosen provisions with the aim of suggesting future considerations for decluttering the black letter law *vis-à-vis* cybercrime.

1. DATA, METHODS AND THE LAW

Literature on cybercrime related criminal law in Estonia is sparse (Sootak 1997, Hirsnik 2014). Computer-related offences were first established in Estonian criminal law in 1997, when the adoption of the Databases Act introduced special offence descriptions to the Criminal Code based on European Union recommendation R(89)9 of 13 September 1989 (Sootak, 1997). Since the coming into force of the Penal Code (PC) on 1 September 2002 (Penal Code, 2001), offence descriptions for computer-related offences have seen important changes multiple times, namely in redactions that came into force on 24.03.2008 and 01.01.2015. These changes came about with the ratification of the Council of Europe's Convention on Cybercrime (Convention, 2004) and the EU Directive on attacks against information systems (Directive, 2013). In the course of 15 years, the number of registered cybercrimes has remained remarkably low. From 2003 to 2018 (Ministry of Justice, 2019, p. 66), only 181 registered cases of interference with computer data (PC §206: the attacks against data provision; Directive Art 5, Convention Art 4), 78 cases of illegal interference with computer systems (PC §207: the disruption provision; Directive Art 4, Convention Art 5), 91 cases of preparation of a computer-related offence (PC §216[1]: the preparation provision; Directive Art 7, Convention Art 6) and 513 cases where access to a computer system was obtained illegally (PC §217: the illegal access provision; Directive Art 3, Convention Art 2). Nevertheless, recent years (2015-2018) have seen a noticeable uptick in registered cases (Ministry of Justice, 2019, p. 66). While an increased number of registered offences does not guarantee an increase in relevant case law, it provides a reason to take a closer look at currently available decided cases.

The case law data for the present study was collected from the Estonian National Gazette (Riigi Teataja) law database, which also includes a search option for court judgements and decisions. The performed search was limited to judgements and decisions made on or after 01.01.2014 and used the term "KarS §2**", i.e. the official abbreviation of the PC in Estonian, in the "text of the case" ("lahendi tekst") search field as the provision-based search option for the database is non-functioning. This required manually reviewing each potential case for suitability. The

search was repeated four times, one for each provision pertaining to computer-related offences (PC §206, §207, §216[1] or §217). Collected judgements and decisions were further filtered to account for one judgement or decision describing multiple offences. The final sample comprised 42 judgements and decisions, where seven cases mentioned more than one of the four provisions. Detailed analysis of the substantive proximity of the provisions is presented in Section 3.

For each case in the final sample (N=42), the case number, date of the judgement or decision, the description of the act where available, and notes on whether PC §213 was included in the judgement or decision were extracted (See Table 1).

TABLE 1: CASES MARKED WITH 'X?' INCLUDED A DISCUSSION OF THE MARKED PROVISION. (X) marks the corresponding provision of the Penal Code in force after 01.01.2015.

Case no.	Date of judgement or decision	§206	§207	§2161	§217	Did the indictment also include §213 (computer-related fraud)?
1-13-7311	09.06.14			X		X
1-14-1081	05.02.14			X		
1-14-3029	31.03.15				X?	
1-14-3276	22.04.14			X		
1-14-3919	28.05.14			X		
1-14-4596	10.06.14			X		X
1-14-5312	04.07.14		X			
1-14-6295	24.09.14			X		X
1-14-6731	14.08.14			X		X
1-14-7403	19.09.14			X		
1-14-9398	19.11.14			X		
1-15-157	29.01.15				X	
1-15-2520	31.03.15			X		
1-15-2640	20.06.17			X		X
1-15-4923	02.09.15			X		
1-15-509	15.04.16		X			
1-15-7057	01.09.15				X	
1-15-8676	09.11.15	X			X	
1-15-8782	02.12.15				X	

TABLE 1: CONTINUED

1-16-11609	14.02.17	X				
1-16-3392	18.05.16	X			X	
1-16-4479	28.02.17	X				
1-16-4515	14.06.16				X	
1-16-636	07.03.16	X			(X)	
1-17-10795	30.11.17		X			
1-17-5454	13.07.17			X		
1-17-6114	21.07.17		X		X	
1-17-8208	25.09.17		X	X	X	
1-18-1220	21.03.18			X		
1-18-3022	08.11.18	X				
1-18-3767	08.10.18			X		X
1-18-6408	30.11.18			X		
1-18-7073	26.09.18			X		X
1-18-827	08.02.18	X				
1-18-830	19.02.18	X				X
1-18-9335	19.12.18			X		
1-19-1662	03.04.19				X	X
1-19-1669	13.03.19			X		
1-19-2202	11.04.19	X			X	
1-19-3674	20.05.19			X		X
3-1-1-93-15	20.11.15				X?	
3-1-1-94-14	22.06.15	(X)	(X)		(X)	

Qualitative content analysis (Kuckartz, 2019) was performed on the extracted action descriptions. Firstly, it was noted whether the case involved only one perpetrator or multiple ones, establishing categories "individual perpetrator" and "multiple perpetrators". The second round of coding noted the specific acts the perpetrators had committed, e.g. "*inserted another person's password"* or "*changed the content of the website*". From this, two categories emerged, namely "technically advanced" and "technically simple" acts. Further, the indictments and lines of argumentation were analysed to establish the context within which the perpetrator(s) committed their acts. Two main context categories that emerged were "personal" and "property-related". Under the

"personal" category, two sub-categories could be distinguished, namely "romantic relationship" and "work-related" sub-categories. Regarding the "property-related" category, it must be clarified that pursuant to the PC, all computer-related offences are legally categorised as offences against property. However, there is a contextual difference between cases where another person's password is entered to gain access to their email account with the purpose of reading their messages or when a password is entered to gain access to someone's online bank account. This distinction prompted another categorisation of the acts according to the purpose with which these were committed. The resulting categories of purpose were "to obtain illicit gains" and "to disrupt or destroy". The results of the qualitative content analysis based on the aforementioned categories, including any relevant overlapping and co-occurrence, is presented in the following section.

2. FINDINGS

The presentation of the results follows from the first round of coding, i.e. separating committed offences based on whether one or multiple perpetrators were involved. The analysis begins with offences involving multiple perpetrators due to the relative uniformity present in these cases. Case law pertaining to offences that only involved one perpetrator had more variation in terms of acts, intent and context. For the purposes of analytical clarity, the individual perpetrator sub-section presents findings based on the context within which the crimes were committed, i.e. "work-related", "romantic relationships" and "other predatory offences".

2.1 MULTIPLE PERPETRATORS

The main distinguishing factor between cases involving multiple perpetrators was whether the committed crimes were technically advanced or not. The largest single stream of similar cases involved the placement and use of "skimmers". Skimmers are devices affixed to ATM machines with the purpose of secretly obtaining debit and credit card information from the card's magnetic strip when people use the ATM. More recently, the use of a specific type of skimmer called a "shimmer" has been witnessed. Shimmers are referred to as such, because it acts as a shim that sits between the chip on the card and the chip reader in the ATM (Krebs, 2015). This difference is significant due to the type of payment cards used in various parts of the world. Europe has been using payment cards with integrated chips a lot longer than in the United States. Although the chip itself cannot be copied, the information from the magnetic stripe remains available for the perpetrators (MacDonald, 2017). Hence, that information can still be used to create payment cards for illegal use where the cards are only 'swiped' for verification. In the sample cases, the typical offence involving the placement and use of skimmers had two perpetrators working in tandem, placing the skimmers onto ATMs along with cameras to record legitimate users entering their PIN-codes. Analysis of the cases revealed that perpetrators were detained at various stages of committing the offence. While some were detained prior to completing the placement of the skimmer itself (Case 1-14-1081), others had already placed the skimmer, copied the data and used payment cards

created with the stolen information to also withdraw cash (Case 1-14-6731). Nine cases that centred on the use of skimmers were decided in Estonian courts in between 2014-2015 and only one in 2018. This could be indicative of how certain modus operandi are used in waves or trends, i.e. during certain periods of time, one cybercrime or another is trending compared to others. Additionally, the indictments lacked information on whether the perpetrators had created and fashioned the skimmers themselves or obtained them from third parties. The use of skimmers, and hence almost a quarter of the total cases, can be categorised as technically simple. Clients of the bank also reported suspicions about there being something wrong with the ATMs (Case 1-14-3276) and increased police surveillance was enough to catch perpetrators in the act.

My analysis indicates that only a few offences exhibited more sophistication either in terms of technical knowledge or organising the operations of the group. In fact, two significant types of cases were revealed through my analysis. On the one hand there was the Ghost Click case (Hacquebord 2011), i.e. case 3-1-1-94-14, and on the other hand, there were cases where crime groups were laundering money or obtaining large quantities of credit card information and perpetrating computer fraud by purchasing goods or services in online stores (Cases 1-15-2640, 1-15-4923, 1-18-6408, 1-18-9935), i.e. cases with a strong connection to the 'kinetic' in terms of criminal proceeds. In case of the former, advanced technological knowledge was employed, whereas the latter exhibited a very specific distribution of tasks among the members of the group even though the cybercrime itself was not technically sophisticated.

The first, technologically more advanced offence appeared in the Ghost Click case (3-1-1-94-14). Central to the offence was malware called DNS-Changer, which was spread to at least four million computers globally. DNS-Changer allowed the perpetrators to control the victimised computers' DNS settings and re-route users to websites determined by the offenders. Illegal gains were obtained from online marketing and advertising platforms, because users whose systems had been infected with DNS-Changer were re-routed to websites displaying certain advertisements. The Ghost Click operation ran for five years from 2006 to 2011, netting the perpetrators upwards of $22M. Whereas the setup was more complicated in comparison to the other cases in the sample that involved multiple offenders, the most disturbing observation in connection to the

Ghost Click case was a legal one. Ghost Click represents a strand of cybercrimes, or borderline cases, that can be called "licensing crimes". Since people are entitled to authorise third persons to impinge on their (property-related) rights, e.g. it is possible to allow someone else to change settings on one's computer or log in to a social media account, licensing agreements presented to people who download software can be used by criminals to prey on unaware computer users. In the Ghost Click case (3-1-1-94-14), software bundling was used to deliver the DNS-Changer malware. The malware was bundled with a media player or video codec and the accompanying licensing agreement stipulated that installing the software might cause changes in the computer's network settings. This possibility of "licensing crimes" presents a significant problem, because most users either do not read the agreements at all (Bakos, Marotta-Wurgler, and Trossen, 2013; Obar and Oeldorf-Hirsch, 2018) or remain confused about the specific legal implications of such agreements after reading them (Cotton and Bolan, 2011).

The crimes of the second group in case 1-15-2640 (the leader) and 1-15-4923 (other members) were two-fold. The first involved using Western Union (WU) money transfers to send criminal proceeds from Japan to Estonia and elsewhere in Europe to be withdrawn and delivered by money mules (Cases 1-15-2640, 1-15-4923). Additionally, the leader of the group had also obtained credit card information from unknown sources and used this information to make at least 39 illegal purchases in various online stores. The obtained goods were often bought in the name of other group members and then retrieved from post offices. Similar methods were used in cases 1-18-9335 and 1-18-6408, where criminal proceeds from computer-related fraud committed in Germany were used to purchase goods, repackage them and then ship the goods to Estonia to be retrieved by the perpetrators. According to the indictment, the illegally purchased goods were so numerous that some were even stored in the home of a grandmother of one perpetrators' grandmothers (Case 1-18-9335).

In general, offences including multiple perpetrators were geared towards obtaining illicit gains. The distinguishing factors between different ways of committing the offences came down to technological and organisational, including legal, sophistication of the operations.

2.2. AN INDIVIDUAL PERPETRATOR

Offences involving multiple perpetrators were solely geared towards preying on unaware victims, i.e. 'crime had to pay' for it to be undertaken. In contrast, the variation of motives and approaches contained in cases involving an individual perpetrator was significant. Hence, the analysis will follow from the context within which the offences were committed. The categories established were "property-related" and "personal", whereas the latter further divided into "work-related" and "romantic relationships".

2.2.1 Work-related

The second noticeable context where offending occurred pertained to work-related situations, which occurred four times in the sample. For example, in Case 1-18-3022, an accountant who had been using a company provided laptop computer for work-related activities maliciously deleted data and materials required by the company to fulfil certain legal obligations. The materials included documents collected in preparation for an audit, different payment schedules and offers related to the company's clients as well as lease agreement documents. In Case 1-16-4479, an IT contractor providing services to a company had illegally and remotely accessed the computer of his contract partner and taken screenshots of Skype conversations, which the perpetrator later emailed to the company's representative. Although this unauthorised access and data collection was the reason for the offender's conviction, it was not the only disruption caused. Contracting IT services puts the maintenance and administration of certain aspects vital to a company's operations in the hands of third persons. In case these work relationships sour, it is easy for a person with advanced technical knowledge to block access to certain important content and administration tools by changing passwords that allow access. While the perpetrator was acquitted of these offences, the mistake made by the IT contractor was the decision to email the work partner screenshots, audio and video of Skype calls, thus incriminating himself. Similar actions were noticeable in Case 1-16-636, where important evidence for the conviction was also available because the perpetrator went 'one step too far' either due to a lack of self-control or being seemingly oblivious to the possibility of actual prosecution.

Another outstanding work-related case in the sample was Case 1-15-509, where 14 accounts at a public agency were temporarily blocked due to incorrect passwords being entered multiple times. To commit the offence, the perpetrator must have had specific knowledge about accessing the information system in question. The offender had masked their IP by using the Tor network and although circumstantial evidence pointed to a specific former employee, the accused was acquitted because the prosecution failed to properly attribute the attacks. The former employee in question had previously worked for the public agency, had been confrontational with many other employees in the past and supposedly had revenge as the motive for perpetrating the attack. The technical investigation in the case relied heavily on the technical knowledge of the witness from the public agency, who presented necessary system logs and other relevant information. However, the case ultimately fell through due to minute inconsistencies between the times of the attacks and the times when the alleged perpetrator had opened a connection to the Tor network. Hence, publicly available technical tools are often enough to avoid being convicted even if most circumstantial evidence point to a specific perpetrator. Work-related offences showed both disruption and destruction as the purpose for committing punishable acts. Ex-employees who either did not possess advanced technical knowledge or were oblivious to the possibility of prosecution behaved in a way similar to the "romantic relationship" offenders, i.e. they did not try to hide their actions by technological means or even incriminated themselves by submitting materials to the victim that turned out to be crucial for the subsequent conviction.

2.2.2 Romantic relationships

Squabbles of ex-partners and people seeking "romance" also formed a considerable portion of the sample cases. In Case 1-15-8676, the case was dismissed due to a lack of public interest and negligible guilt. The perpetrator had logged into the victim's e-mail account and Facebook account to read messages contained therein. The request to dismiss the case was based on the fact that the entire situation was a family matter and the accused regrets committing the acts. Another 'tongue in cheek' type of romantic pursuit was discussed in Case 1-19-1662. The perpetrator had illegally obtained access to numerous companies' WiFi routers to use the

SIM-card of the router to connect to special tariff numbers. The numbers to be contacted were related to parking services and websites containing adult content. In Case 1-16-3392, the perpetrator had obtained and used the Gmail password of his ex-partner to access the account. Following that, the offender requested password changes and tied these account recovery requests to an account inaccessible for the ex-partner. Again, the Facebook account of the victim was compromised in the process. Similar acts were perpetrated in Case 1-16-4515, where the perpetrator also took pictures of the other persons conversations. Compromising an ex-partners email and/or social media accounts was a general method of gaining access to information the perpetrator had no longer any reason to be aware of. The most significant case related to ex-lovers was 1-16-636. Here, the perpetrator had not simply obtained the ex-partners passwords to specific accounts but had placed a remote access backdoor on the victim's computer. The software used to perpetrate later offences was EasyBits Kids – a piece of software that is targeted to parents who wish to remotely control their child's online activities and computer use. The perpetrator was not satisfied with merely knowing what the ex-partner was communicating. In addition to reading the messages exchanged between the ex-partner and third persons, the perpetrator verbally abused the ex-partner via text messages, both taunting the victim by admitting to 'hacking the accounts' and making lude comments about the ex-partner's choice of new potential partners. With the exception of the outlier router SIM-card case that can be considered personal by proxy due to the nature of services purchased, all court cases dealing with acts arising from real romantic relationships had disruption as their main purpose for committing the offence. However, the disruption only concerned negatively impacting one person, i.e. the ex-partner.

2.2.3 Other predatory offences

Aside from the "personal" category of offences, "property-related" crimes committed by individual perpetrators varied significantly with no one shared aspect connecting the different acts. For example, in Case 1-17-10795, the accused who was 70 years old at the time of sentencing had used a signal amplifying antenna, his laptop and special software to jam the central device of a radio alarm system. His actions caused significant proprietary damage to the security company and the indictment showed

no specific motivation on behalf of the accused to commit such an act. In general, blocking relevant signals from reaching the alarm devices could be used to temporarily knock out a modern security system, but the case materials show no such intent from the perpetrator. Other cases involved storing and using malware (Case 1-17-6114), storing malware and illegally obtained credit card information on one's computer (Case 1-19-1669) or storing and using illegally obtained credit card information (Case 1-19-3674). While offences that involved an individual perpetrator but did not fit under the "personal" category seemingly have no 'red line' connecting them, these are all opportunistic predatory crimes that have disruption, destruction or proprietary gain as their purpose. Overall, these acts were of a higher technical sophistication than those under the "romantic relationship" category, as the latter are characterised by visceral reactions more so than detailed and poised conduct, i.e. offences in the "romantic relationship" category were perpetrated by any means necessary as long as a certain goal was achieved.

3. LEGAL ANALYSIS

On one hand, the primary problem surrounding cybercrime offences listed in the Estonian PC is simple: many different offence descriptions with identical maximum sentences and minimal differences in their constitutive elements. Yet, this problem is simultaneously difficult to overcome, because the provisions have already been amended multiple times, including important substantive changes in offence descriptions. This legislative indecisiveness was highlighted in Supreme Court ruling 3-1-1-94-14 (p. 175). The court had to admit that the perpetrators would have skated scot free according to an earlier version of a provision, but not according to a later wording – before 24.03.2008, the perpetrators would have had to cause significant damage in order to be prosecuted pursuant to PC §206.

While the precise reason for such legislative ambiguity over the years is not clear, a closer look at the system of provisions in the PC itself provides some insight. In their current form, the four provisions for which case law data was collected have all been incorporated into the PC due to international obligations, derived from a combination of the Council of Europe's Convention on Cybercrime (ETS No. 185) and the EU Directive on attacks against information systems. However, seemingly little thought has gone into establishing provisions that provide adequate legal protection, can withstand the rapidly changing nature of cybercrime and are more readily comprehensible to the professionals applying them, given that these professionals do not necessarily possess specialist technical knowledge. In the following section, all four main provisions and §213 are analysed in turn, ending with §206 that could potentially become the central cybercrime provision if properly modified.

3.1 PC §207 (THE 'DENIAL OF SERVICE' PROVISION; DIRECTIVE ART 4, CONVENTION ART 5)

For PC §207(1) to be applied, the perpetrator has to illegally interfere with or hinder the functioning of a computer system. Leaving aside the

meaning of 'illegal' and 'computer system', the former of which will be addressed below, the deciding judges need to distinguish between interference and hindering. In 3-1-1-94-14, interference and hindering were interpreted to occur when a computer system is not functioning as intended, with interference being less intensive than hindering. Regardless of whether the system under question is relatively simple or highly complex, the wording of §207 requires a judge, and the prosecutor when preparing the indictment, to assess technical questions. Multiple parameters can be used to determine if a system is functioning 'as intended', including technical and cybersecurity standards as well as specific service level agreements. Among other things, this is a burden on the criminal justice system, because it requires additional technical investigation. The primary problem, however, is that the people preparing indictments and delivering decisions do not possess advanced technical knowledge (Ministry of Justice 2019). The reason for the existence of §206 and §207 is that the former deals with attacks 'against data', the latter with attacks against information systems or computer systems. To clarify, Art 1(a) of the Convention speaks of 'computer systems', while the Directive defines 'information system' in Art 2(a), both meaning the functionality achieved from a combination of hardware and software. Attacks against data comprise unlawful or unauthorised data processing activities and are therefore conceptually easy to distinguish, because the emphasis is on determining what is or is not illegal in each case. The processing activity is illegal if no basis for it exists under law or the person engaging in the activity is not authorised to do so by whomever has the right to provide authorisation. Essentially, §207 is a qualification of §206 for cases where, in addition to illegal data manipulation, the activities also affected the proper functioning of an information or computer system. Given that both offences carry an identical sanction, the purpose of their separate existence remains unclear. Furthermore, there are two conceivable ways in which a person can interfere with or hinder the functioning of a computer system. The first option is to use physical force to render the system unusable. If the damage is significant enough, this action would fall under PC §203. The other option is reflected in §207, where a system's functioning becomes affected through receiving some form of transmission, e.g. transmitting arbitrary data to block channels on the receiving device. This activity was present in Case 1-17-10795, where the perpetrator used his laptop, specific software and a signal amplifying antenna to jam, i.e. block other incoming signals, on

an alarm system's central unit, causing significant proprietary damage. Since cybercrime provisions do not explicitly exclude the use of physical force in disrupting the functioning of information systems, but focus specifically on signal transmissions, then a qualifying provision concerning attacks against information systems that carries a maximum sentence identical to an attack perpetrated against data is entirely unnecessary. The manner of achieving the intended results are identical in PC §206 and §207, always initiated by some form of unauthorised (arbitrary) data transmission.

3.2 PC §216[1] (THE 'PREPARATION PROVISION'; DIRECTIVE ART 7, CONVENTION ART 6)

PC §216[1] is the clearest sign that computer-related offences in the PC ought to be considered as stages in an iterative delict. While this notion is certainly obfuscated by the speed with which commission stages of cybercrimes advance from one legally relevant state to another, the iterative nature of the offences can still be gleaned. In Case 1-17-8208, the accused was convicted of offences under PC §216[1], §217 and §207, although the actions of the accused related solely to changing the content of a single website, i.e. altering the text, images and design of the website. The preparation was not broad, because it pertained to placing a remote backdoor to one administrator system, access was illegally obtained by using that same specific backdoor and the final act was website defacement, i.e. malicious alteration of website content. If the preparation was clearly connected and limited to one specific final act, then the reason for also convicting the person under the 'preparation provision' remains unclear, unless the judge and prosecutor (and the defence) failed to understand that the committed individual acts were stages in an iterative delict. To clarify, two significant sequences of offences that possess an iterative nature in the PC are counterfeiting money and cybercrimes. Perhaps the iterative nature of the wrongdoing is easier to grasp in counterfeiting, where the completed act would render it unnecessary to also convict a person under a provision concerning the preparation for the final offence. Based on the sample, there are two primary ways in which an offence under PC §216[1] is committed: being in the possession of or placing a device necessary for copying credit card information at the ATM

or payment terminal (e.g. Case 1-14-6731) and storing illegally obtained credit card information on a data storage medium (e.g. Case 1-19-3674). Other cases involved the possession of user information, i.e. usernames and passwords (Cases 1-15-8782 and 1-16-3392), or malware (Case 1-19-1669). The wording of PC §216[1] requires the prosecution to prove that the perpetrator possessing the device, program or data had the intention of using it to commit an offence. The explanatory report preceding the current version of offence descriptions in the PC (Explanatory Report 554 SE, 2013) stated that previous wordings of the provisions were too vague and could also allow for the prosecuting of cybersecurity experts who are in the possession of malware due to the nature of their daily work, yet lack the intention of committing an offence. The same can be stated about any devices that can, but do not necessarily have to be, used to commit cybercrimes. While the idea behind PC §216[1] is useful with regard to curbing the commission of cybercrimes in earlier stages, it is dysfunctional in practice. This is precisely because the prosecutor always needs additional proof of intention regarding future crime commission that can, for example, manifest in the form of communication pertaining to planned criminal conduct or apprehending offenders in the process of committing the actual crime. Here, the legislator could consider modifying PC §206, i.e. attacks against data, to also include 'obtaining' into the wording. Skimmers, other similar devices, malware as well as illegally obtained 'means of protection', e.g. passwords or credit card information, are all ultimately used for data manipulation. Data manipulation is expressed in specific data processing related actions, such as those listed in Art 4(2) of the General Data Protection Regulation (Regulation, 2016), including collection, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. Following from this comprehensive list, if the perpetrator illegally obtains or intends to obtain data, all of the abovementioned cases are covered and do not require PC §216[1] as a separate provision. In cases where data has been collected already, the modified PC §206 requirements have been fulfilled. In other instances, a case for an attempted attack against data could be presented, if the perpetrators were unable to complete the offence, but had (unsuccessfully) tried to use malware against someone's system or already placed devices such as skimmers without receiving any data.

Although PC §213 (computer-related fraud) was not included in the case law search, it nevertheless was prominent in cases related to PC §216[1] and categorised under acts committed with the aim of obtaining illicit gains. As a *sui generis* derivation from the offence of fraud, i.e. PC §209, the defining characteristic of computer-related fraud is that computers cannot be deceived like humans. There are no other differences between the two offence descriptions, as both prescribe sanctions for causing proprietary damage to another person with the aim of obtaining proprietary benefit from the same act. With the suggested changes to PC §206 and the removal of PC §216[1] altogether, the legislator could consider absorbing PC §213 into the general offence of fraud as the second alternative. For example, the offence of extortion (PC §214) uses a similar construct, employing the alternatives 'threatening to' or 'by use of violence' in explaining how a person must be coerced, or proprietary benefits transferred, to prosecute the conduct as criminal extortion. The illegality of specific acts for which the PC prescribes sanctions would not change, but the law would be decluttered. Furthermore, the nature of fraud has changed in general and, considering Estonian crime statistics (Ministry of Justice, 2019) as well as news regarding major developments in the crime statistics for England and Wales (2018), computer-related fraud is merely a part of the 'new normal'.

3.3 PC §217 (THE 'ILLEGAL ACCESS' PROVISION; DIRECTIVE ART 3, CONVENTION ART 2) AND PC §206 (THE 'ATTACKS AGAINST DATA' PROVISION; DIRECTIVE ART 5, CONVENTION ART 4)

Illegally obtaining access to a computer system by removing or circumventing a protective measure has thus far been considered the 'central' cybercrime provision (Case 3-1-1-94-14, p 186). Obtaining access to a computer system is part and parcel for committing many cybercrimes, but there were numerous cases in the sample which did not require 'using' the system to be successfully perpetrated. To consider something as central would require the phenomenon to manifest in each case and, based on the sample, that is not true for PC §217. For example, jamming signals (e.g. Case 1-17-10795) or committing DDoS attacks do not require access

to the system in order to negatively affect it. Stolen credit card information can be obtained from other perpetrators (e.g. Case 1-18-9335), from anonymous communication via darkweb marketplaces (Case 1-15-2640), but could also be obtained through deceptive acts such as *phishing*, i.e. employing social engineering tactics to convince victims to hand over their data either via email, fake websites or fraudulent links in SMS messages. Furthermore, both 'removal of' and 'circumventing' the means of protection by digital means is already an attack against data. In the cases analysed, removal of a protective measure meant either the unauthorised insertion of a password (e.g. Cases 1-15-8782 and 1-16-3392) or a credit card number (e.g. Cases 1-13-7311 and 1-15-2640). Circumventing a protective measure was achieved by installing a backdoor into the system (Case 1-17-8208). With the former, if passwords or credit card information has been illegally obtained, it is already an attack against data. If the passwords are then used, then the violation is simply more intense, and in case unauthorised credit card use occurs, then we must move on to analysing an attempted or concluded offence of (computer-related) fraud. Unauthorised use of a means of protection can be considered as illegal interference with computer data, because the person either should not have been in possession of it in the first place (i.e. obtaining is illegal) or, knowing it does not belong to him or her, should not have used it. In a technical context, circumventing a protective measure requires some form of unauthorised data transmission to occur, e.g. trying to infect or successfully infecting a system with malware, which means that the act prior to obtaining access was already illegal. This is a major reason why augmenting PC §206 ought to be considered by the legislator. Plenty of questionable actions take place before access to a system is obtained, if obtaining access in the strict sense is necessary at all. By creating a central 'attacks against data' provision, there would be no need for:

- §217: obtaining access is already data manipulation.

- §207: interfering with or hindering the functioning of a computer system affects accessibility to data contained therein and is thus an attack against data in the form of restricting access.

- §216[1]: when unauthorised data collection has occurred, an 'attack against data' has been committed, and attempting to collect data

without a legitimate reason is also an attempted attack against said data.

Although this would not apply to its current wording, the central cybercrime provision in the PC ought to be §206, i.e. attacks against data. Using the comprehensive list of data related actions available from the GDPR would allow flexibility in applying the provision. The key aspects to prove and assess in court would be whether the data related action was illegal or not. This would shift the analysis back towards legal questions and away from complex technical descriptions. According to the current test, illegality of an action can be confirmed if there is no provision allowing it or the action has not been authorised by a person entitled to do so. Since all of the current computer-related offences require intent from the perpetrator, mishaps or human error (negligence) are excluded from viable cases. The perpetrator must have envisioned his or her actions prior to committing them. The proximity of the four provisions mechanically spreads out legally relevant acts that are very closely related if not entirely the same, i.e. all pertain to attacks against data one way or another. The provisions also exclude physical attacks (see section 3.1 about PC §203) and only implement a machine-like distinction between an information system and data. This speaks more to the inadequate amount of thought given to formulating the provisions upon adoption into domestic law rather than a specific legal or social need to make such distinctions. The issue does not stem from the international origin of the provisions, but a lack of domestic assessment regarding the severity of such offences and whether these different punishable acts should carry different maximum sentences. A clear example here is the distinction between §206 and §207. The latter is supposedly a qualification of §206 that ought to carry a heavier sentence, yet both offences carry a maximum sentence of three years imprisonment (Hirsnik, 2014). Since §217, i.e. the illegal access provision, also carries a maximum sentence of three years imprisonment, assessing the way in which the legislator has (or has not) analysed the injustice embedded into these punishable acts is difficult. If the current maximum sentences are retained, then combining §206, §207 and §217 into a single provision is recommended, given the substantive proximity of these provisions.

As shown above with Case 1-17-8208 (Section 3.2) and considering this similarly holds true for cases involving PC §216[1] followed by PC §213 (e.g.

Case 1-19-3674), the courts do not really distinguish between the legal significance of offences that correspond to the preparation provision followed by a delict damaging someone's rights. The preparation provision ought to be evoked only when there is no further damage caused (Sootak and Pikamäe, 2015, §216[1]). It is the same for both computer-related fraud perpetrated with the use of stolen credit card information and skimmer cases. Once the perpetrator(s) commence(s) actions that can be considered as corresponding to fraud, or any other computer-related offence, the preparation provision should no longer be used, and an attempt of the damaging offence should be analysed instead. Furthermore, the application of PC §216[1] in its current form is limited, because it cannot be used in cases involving *phishing* where the perpetrators are not after credit card information or passwords. However, these instances can be equally damaging, for example when people disclose personal information or facts to offenders who have no legal basis for requesting such information.

The current cybercrime provisions in the PC are used rarely, and in more complicated cases, their application relies heavily on witnesses who possess advanced technological knowledge.

CONCLUSION

The study was undertaken to obtain a better understanding of the Estonian cybercriminal in action based on court judgements and decisions available from 2014-2019. Although the sample of cases was small (N=42), interesting patterns were gleaned from the judgements and decisions analysed.

For the most part, crimes involving multiple offenders were distinguishable solely based on the level of technological and organisational sophistication employed, since all such crimes were motivated by proprietary gains. In contrast, individual perpetrators varied significantly in terms of crime contexts and motivations for the offences. When the offences involved ex-partners of a past romantic relationship, the perpetrators used any means necessary to covertly observe the actions and communications of their ex-partner. Individual perpetrators committing offences determined as "personal" also showed a tendency for self-incrimination by taunting the victim or forwarding them materials that were later used as permissible evidence. Predatory crimes outside the "personal" category were opportunistic and varied significantly in technological sophistication. Such offences also had no shared aspect in terms of the underlying motivation for committing the crimes.

Convictions in many of the cases, e.g. the use of skimmers, stemmed from the possibility of observing the perpetrators in action or even receiving relevant hints from regular people. In at least two cases, convictions were possible because the perpetrators had communicated materials to the victims that could later be used as evidence in court. More complicated cases seemed to rely heavily on evidence provided by other law enforcement agencies or witnesses who possessed advanced technical knowledge.

The findings of the above socio-legal analysis indicate that in terms of substantive criminal law in Estonia, the current system of provisions analysed in the article includes offences that are substantively very closely related and is thus more a result of machine-like adoption of international instruments rather than following from the thoroughly

analysed essence of cybercrimes. Whether related to romantic relationships, work or illegally obtaining proprietary gains, the perpetration of 'true cybercrime' is really only focussed on causing real-world impact through data manipulation and thus the legal provisions enacted to protect against these infractions ought to reflect the notion properly and clearly. The current mechanical distinction between offence descriptions that are indeed very closely related in terms of substance is entirely unnecessary, which can primarily be gleaned from such a small number of cases for each separate provision as well as the fact that the provisions often appear together in the indictments.

Contact:

Kristjan Kikerpill
E-mail: kristjan.kikerpill@gmail.com

REFERENCES AND SOURCES

Atkins, B. and Huang, W. (2013) 'A Study of Social Engineering in Online Frauds', *Open Journal of Social Sciences*, 1(3).

Bakos, Y., Marotta-Wurgler, F., and Trossen, D. R. (2014) 'Does Anyone Read the Fine Print? Consumer Attention to Standard Form Contracts', *New York University Law and Economics Working Papers*, 195.

Bossler, A. M., and Holt, T. J. (2009) 'On-Line Activities, Guardianship, and Malware Infection: An Examination of Routine Activities Theory', *International Journal of Cyber Criminology*, 3(1).

Case 1-13-7311, 09 June 2014.

Case 1-14-1081, 05 February 2014.

Case 1-14-3726, 22 April 2014.

Case 1-14-6731, 14 August 2014.

Case 1-15-2640, 20 June 2017.

Case 1-15-4923, 02 September 2015.

Case 1-15-509, 15 April 2016.

Case 1-15-8676, 09 November 2015 (decision).

Case 1-15-8782, 02 December 2015.

Case 1-16-3392, 18 May 2016.

Case 1-16-4479, 28 February 2017.

Case 1-16-4515, 14 June 2016.

Case 1-16-636, 07 March 2016.

Case 1-17-10795, 30 November 2017.

Case 1-17-6114, 21 July 2017.

Case 1-17-8208, 25 September 2017.

Case 1-18-3022, 08 November 2018.

Case 1-18-6408, 30 November 2018.

Case 1-18-9935, 19 December 2018.

Case 1-19-1662, 03 April 2019.

Case 1-19-1669, 13 March 2019.

Case 1-19-3674, 20 May 2019.

Case 3-1-1-94-14, 22 June 2015. Supreme Court of Estonia (Criminal Chamber).

Cotton, H., and Bolan, C. (2011) User Perceptions of End User License Agreements in the Smartphone Environment, *Proceedings of the 9th Australian Information Security Management Conference*, 05-07 December. Perth, Western Australia.

Convention on Cybercrime. (2004) Council of Europe Treaty No. 185, 01 July.

Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA. (2013) *OJ L 218, 14.8.2013*.

Dizon, M. (2016) 'Breaking and Remaking Law and Technology: A Socio-techno-legal Study of Hacking', *Doctoral Thesis*. [Online source] Available from: https://pure.uvt.nl/ws/portalfiles/portal/12403280/Dizon_Breaking_28_06_2016.pdf [Accessed 31.08.2019].

European Commission. (2017) *Special Eurobarometer 464a: Europeans' Attitudes Towards Cyber Security*.

Explanatory Report SE 554. (2013) *Karistusseadustiku muutmise ja sellega seonduvalt teiste seaduste muutmise seadus 554 SE*, 09 December 2013.

Felson, M., and Boba, R. L. (2010) Crime and Everyday Life, 4th Ed. Sage Publications.

Gallagher, S. (2019) 'Ransomware strike takes down 23 Texas local government agencies', *Ars Technica*. [Online source] Available from: https://arstechnica.com/information-technology/2019/08/ransomware-strike-takes-down-23-texas-local-government-agencies/ [Accessed 31.08.2019].

Newman, L. H. (2018) 'Atlanta spent $2.6M to recover from a $52 000 ransomware scare', *Wired*. [Online source] Available from: https://www.wired.com/story/atlanta-spent-26m-recover-from-ransomware-scare/ [Accessed 31.08.2019].

Hacquebord, F. (2011) 'Esthost Taken Down – Biggest Cybercriminal Takedown in History', *Trend Micro*, 09 November. [Online source] Available from: https://blog.trendmicro.com/trendlabs-security-intelligence/esthost-taken-down-biggest-cybercriminal-takedown-in-history/ [Accessed 31.08.2019].

Heller, N. (2017) 'Estonia, the Digital Republic', *The New Yorker*, 11 December. [Online source] Available from: https://www.newyorker.com/magazine/2017/12/18/estonia-the-digital-republic [Accessed 31.08.2019].

Hirsnik, E. (2014) 'Arvutikuritegevuse regulatsioon Eestis: karistusõiguse revisjoniga toimunud muudatused ja lahendamata jäänud probleemid', *Juridica*, VII.

Hutchings, A., and Hayes, H. (2009) 'Routine Activity Theory and Phishing Victimization: Who Gets Caught in the 'Net'?'. *Current Issues in Criminal Justice*, 20 (3).

Kikerpill, K., and Siibak, A. (2019) 'Living in a Spamster's Paradise: Deceit and Threats in Phishing Emails', *Masaryk University Journal of Law and Technology*, 13(1).

Krebs, B. (2015) 'Chip Card ATM 'Shimmer' Found in Mexico', *KrebsOnSecurity*, 11 August. [Online source] Available from: https://krebsonsecurity.com/2015/08/chip-card-atm-shimmer-found-in-mexico/ [Accessed 31.08.2019].

Kuckartz, U. (2019) Qualitative Text Analysis: A Systematic Approach. In: Kaiser G., Presmeg N. (eds) Compendium for Early Career Researchers in Mathematics Education. ICME-13 Monographs. *Springer: Cham*.

MacDonald, J. (2017) 'The New Card Skimming is called 'Shimming'', 03 May. [Online source] Available from: https://www.creditcards.com/credit-card-news/new-card-skimming-is-called-shimming.php [Accessed 31.08.2019].

Lavorgna, A. (2015) 'The Online Trade in Counterfeit Pharmaceuticals: New Criminal Opportunities, Trends and Challenges', *European Journal of Criminology*, 12(2).

LexisNexis Risk Solutions. (2019). EMEA Cybercrime Report.

Leukfeldt, E. R. (2014) 'Cybercrime and Social Ties. Phishing in Amsterdam', *Trends in Organized Crime*, 17(4).

Leukfeldt, E. R., and Jansen, J. (2015) 'Cyber Criminal Networks and Money Mules: An Analysis of Low-Tech and High-Tech Fraud Attacks in the Netherlands', *International Journal of Cyber Criminology*, 9(2).

Leukfeldt, E. R., and Yar, M. (2016) 'Applying Routine Activity Theory to Cybercrime: A Theoretical and Empirical Analysis', *Deviant Behavior*, 37(3).

McGuire, M. 2018. Into the Web of Profit – Understanding the Growth of the Cybercrime Economy. *Bromium*.

Ministry of Justice, Republic of Estonia. (2019) *Kuritegevus Eestis 2018*.

Obar, J. A., and Oeldorf-Hirsch, A. (2018) 'The Biggest Lie on the Internet: Ignoring the Privacy Policies and Terms of Service Policies of Social Networking Services', *Information, Communication & Society*, DOI: 10.1080/1369118X.2018.1486870.

Penal Code. (2001) 2001/61, 364, Estonia: *Riigi Teataja* (State Gazette). In Estonian. English translation. [Online Source] Available from: https://www.riigiteataja.ee/en/eli/509072018004/consolide [Accessed 31.08.2019].

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). *OJ L 119, 4.5.2016*.

Reynolds, M. (2016) 'Welcome to E-stonia, the World's Most Digitally Advanced Society', *WIRED*, 20 October. [Online source] Available from: https://www.wired.co.uk/article/digital-estonia [Accessed 31.08.2019].

Reyns, B. W. (2013) 'Online Routine and Identity Theft Victimization: Further Expanding Routine Activity Theory Beyond Direct-contact Offenses', *Journal of Research in Crime and Delinquency*, 50(2).

Sootak, J., and Pikamäe, P. (2015) Karistusseadustik: kommenteeritud väljaanne (The Penal Code: Commented Edition), *Juura*: *Tallinn*.

Soudjin, M. R. J., and Zegers, B. C. H. T. (2012) 'Cyber Crime and Virtual Offender Convergence Settings'. *Trends in Organized Crime,* 15(2-3).

Torbet, G. (2019) 'Baltimore ransomware attack will cost the city over $18 million', *Engadget*, 06 June. [Online source] Available from: https://www.engadget.com/2019/06/06/baltimore-ransomware-18-million-damages/ [Accessed 31.08.2019].

Van Hoecke, M. 2011. Legal Doctrine: Which Method(s) for What Kind of Discipline? *in* van Hoecke, M (Ed). Methodologies of Legal Research – Which Kind of Method for What Kind of Discipline? *Hart Publishing*.

Wall, D. S. (2008) 'Cybercrime, Media and Insecurity: The Shaping of Public Perceptions of Cybercrime', *International Review of Law, Computers and Technology*, 22(1-2).

DEVELOPMENT AND PREVENTION OF JUVENILE FIRE-RELATED RISK BEHAVIOUR IN THE SOCIAL LEARNING PROCESS

Margo Klaos (corresponding Author), MA
University of Tartu, Institute of Social Studies
PhD student
Estonian Rescue Board
Head of Southern Rescue Centre

Diva Eensoo, PhD
University of Tartu, Department of Family Medicine and Public Health
Analyst

Kadi Luht-Kallas, MSc
University of Tartu, Department of Education
PhD student
Estonian Academy of Security Sciences, Rescue College
Lecturer

Jaanika Piksööt, MSc
National Institute for Health Development, Tallinn
Analyst

Keywords: fire-play, fire setting, risk behaviour, fire prevention, social learning, school

ABSTRACT

Playing with fire is the most common cause of fire death among children. Although many previous studies have focused on socio-demographic predictors of childhood fire deaths and pathological fire-setting behaviour, less attention has been paid to how the fire-related risk behaviours develop and how they can be reduced by involving schools.

The aim of our research was to determine the main personal and environmental variables shaping children's fire-related risk behaviour during the social learning process. The study was carried out in Estonia with a sample of 903 students from sixth grade classes. We analysed the children's safety knowledge, experiences, social environment, and safety education at school compared to their declared frequency of fire-play.

The study emphasizes the high prevalence of fire-play among students aged 12. We concluded that the most significant predictors of children's high-risk fire-play were: being a boy, living separately from parents, lower fire safety knowledge, history of fire accidents, previous use of fire, parents' unsafe behaviour at home, parents not being role models of safety, and a lower interest to learn safety issues. It is important to consider these risk factors when planning appropriate interventions for fire prevention.

We conclude that in order to equally reach all risk groups it is necessary to develop the schools as community centres of youth injury prevention. We emphasize that schools should have a special role of compensating the deficiencies of knowledge, attitudes, skills, and social network to reduce the youth risk behaviour caused by social inequalities.

INTRODUCTION

Fires are the leading cause of death from injuries at home in children, and such deaths are concentrated in the most deprived populations (Sethi et al., 2008, p.49). Fire-play is the predominant cause of residential fire related injuries and deaths among young children (Istre et al., 2002, p.131). The most common fires that result in the death of a child are started by children, and often the child kills themselves through fire-play (Harpur, Boyce & McConnel, 2013, p.73). The reason for this is mainly their lower cognitive capacity and higher physiological vulnerability. Their curiosity and wish to experiment are not always matched by their capacity to understand or respond to danger. (Istre et al., 2002; Towner & Scott 2008, p8; Harpur, Boyce & McConnel, 2013).

In the literature, the children's fire-related behaviour is often divided into two types: fire-play and fire-setting. The differentiation between these derives from the level of intent and malice. The term fire-play is often used to convey a low level of intent to inflict harm and an absence of malice. Fire-setting is used to describe a higher level of intent. They are also divided based on the age of the children. Younger children usually play with fire because of curiosity or a wish to experiment (fire-play). Youth in their early teens are more involved in intentional and malicious behaviour (referred to as firesetting). Fire-play is usually defined as any form of misuse of fire materials by youth, notably: matches, lighters, and firecrackers, without parental permission or supervision. (Kafry, 1980, p.2; Putnam & Kirkpatrick, 2005, p.2; Hall, 2010, p.6; Harpur, Boyce & McConnel, 2013, p.73).

Experimentation with fire often begins in early childhood, and fire play typically peaks in late childhood or early adolescence (Fessler, 2006, p.429). It has been found that children's highest level of recent fire play is reported at the age of 12, which constitutes the dangerous apex of the combination of factors: willingness to obey rules, more opportunities outside adult supervision, access to sources of ignition, and incomplete mastery of controlling fire (Fessler, 2006, p.437; Grolnick et al 1990, p.131).

The fire fatalities among children are deeply related to one of the central concerns of demography and sociology – the profound inequities of mortality in society (Shai & Lupinacci, 2003). Different studies (Roberts & Power, 1996; Towner & Warda, 1998; Shai & Lupinacci, 2003; Edelman, 2007; Harpur, Boyce & McConnel, 2013) have pointed out the steep social gradient for childhood deaths from house fires. The main factors that raise the risk of fire-setting behaviour and higher mortality are a lower quality of their physical and social environment. They have concluded that the main family factors that predict the increased risk of child fire death or burn injury are: 1) poverty, combined with poor housing conditions and social isolation; 2) single parents; 3) lack of parental education; 4) parent's smoking; 5) inadequate supervision; 6) large families; 7) lack of a functioning smoke alarm. (Towner & Warda, 1998, p.23; Edelman, 2007, p.963; Hall, 2010, p.40; Shai & Lupinacci, 2003, pp.115-122; Harpur, Boyce & McConnel, 2013, p.73; Jennings, 2013, pp.2-4).

Fire-play is also related to problem areas in the children's lives. Children who are involved in fire-play show a higher incidence of different behavioural problems. Child, parent, and family dysfunction increase interpersonal problems and limits positive family interactions that may decrease children's involvement in deviant behaviour. (Kafry, 1980, p.14; Kolko, 2001, p.359; Harpur, Boyce & McConnel, 2013, p.77). Various characteristics of problematic firesetting tend to develop in those who have been inadequately supervised and those with high levels of individual and family psychopathology (Dolan et al., 2011, pp.391).

Most of the main risk factors are difficult to change and therefore need to be considered when designing prevention programs. As children get different social capital and background from home, schools have an important role to play. Bandura (2004, p.158) has argued that it is easier to prevent detrimental health habits than try to change them after they become part of a lifestyle. Prevention of childhood residential fire-related deaths requires much more than a smoke alarm installation program and should be based on the interventions to prevent fire-play in order to be successful (Istre et al., 2002). Possible means of preventing fire-play related injuries include educational programs aimed at children and parents to balance the protective devices and educational efforts (Dietrich, 1952; Istre et al., 2002; Harpur, Boyce & McConnel, 2013). Bandura (2004) points out the very important role of schools in promoting public

health because children can be easily reached. Dougherty et al. (2007) also propose that school-based programs should play an important part in the effort to reach not only the children in the classroom, but also their parents. Most of the previous studies (Towner & Warda, 1998; Istre et al., 2002; Shai & Lupinacci, 2003; Edelman, 2007; Hall, 2010; Harpur, Boyce & McConnel, 2013) have mainly analysed the family-related risk factors of children's fire-play or pointed out the idea that children and parents need special education programs to reduce the fire-play of children; but the certain role of schools is not usually proposed.

Bandura (2004, pp.157-158; 1998, pp.19) has discussed that many of the lifelong habits that jeopardise health are formed during childhood and adolescence, and rooted in familial practices. The social environment has an important influence to the development of children's behaviour during the social learning process. Bandura's (1971) Social Learning Theory gives a good framework to analyse the impact of the social environment on the children's fire-related risk behaviour, and can be used to design school-based fire prevention programs.

The social learning theory extends the learning process beyond the educator-learner relationship to the larger social world; and explains the socialisation process as well as the breakdown of behaviour in society (Braungart & Braungart, 2007, p69). It also explains human behaviour in terms of unidirectional causation, in which behaviour is shaped and controlled either by environmental influences or by internal dispositions (Bandura, 2001). Bandura (2001, p.2) argues that personal factors, behavioural patterns, and environmental events all operate as interacting determinants that influence each other bidirectionally (Figure 1). The theory emphasizes reciprocal determinism in the interaction between people and their environment. It posits that human behaviour is the product of the dynamic interplay of personal, behavioural, and environmental influences. Environmental factors influence individuals and groups, but individuals and groups can also influence their environment and regulate their own behaviour. (McAlister, Perry & Parcel, 2008, pp.170-171). The theory turns attention to the impact of social factors and social context within which learning and behaviour occur (Braungart & Braungart, 2007, p.67). Environmental events in the form of modelling, instruction, and social persuasion affect the person, and the person in

turn evokes different reactions from the environment, depending on his or her personality and physical features. (Grusec, 1992, pp.782-783).

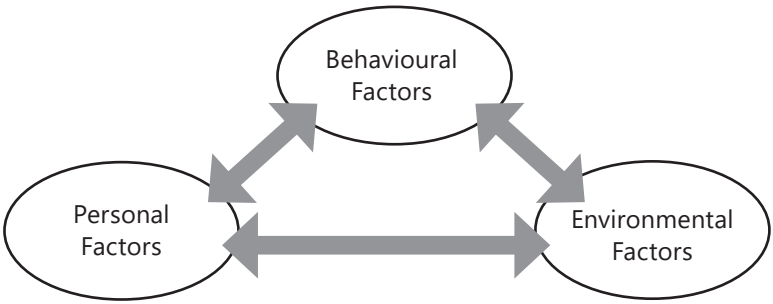


FIGURE 1. Model of triadic reciprocal determinism of social learning theory (Bandura, 1989, p.3).

In the social learning system, new patterns of behaviour can be acquired through direct experience, through social modelling by observing the behaviour of others, or through verbal persuasion (Bandura, 1971, p.3; Rosenstock, Strecher & Becker, 1988, p.180; McAlister, Perry & Parcel, 2008, pp.176-177). This approach emphasizes the importance of exploratory experiences, and imparting of information by social agents in the form of guided instruction and modelling, as a source of change (Grusec, 1992, p.784). Performance accomplishments are the most influential sources of efficacy information because they are based on personal mastery experience. On the other hand, this rudimentary form of learning is largely governed by the rewarding and punishing consequences that follow any given action. Vicarious experience obtained through observation of successful or unsuccessful performance of others is the next most potent and, indeed, may account for a major part of learning throughout life. Verbal persuasion (or exhortation) is frequently used in health education; while it is less powerful than performance accomplishments or vicarious experience, it can still be a useful adjunct to more-powerful influences. (Rosenstock, Strecher & Becker, 1988, p.180; Bandura, 1971, p.3; Bandura, 1977, pp.195-196).

Although many previous studies have focused on socio-demographic predictors of childhood fire death or pathological fire-setting behaviour, less attention has been paid to how the fire-related risk behaviour

develops and can be reduced in the social learning process. The aim of this paper is to determine the main personal and environmental variables influencing and shaping children's fire-related risk behaviour during the social learning process. To reach the goal we compare the children's fire-related behaviour with their safety knowledge, personal experiences, everyday social environment, and safety education at school according to Bandura's (1971) Social Learning Theory. Based on the survey, we argue and intend to make suggestions on how to teach fire safety at school to compensate for deficiencies in children's social learning process.

1. METHODS

1.1 SAMPLE

The current article is based on the study "The Effectiveness of Health Promotion in Estonian Schools". This study was carried out in the school year 2012/2013 in Estonia. The sample was randomly selected sixth-grade students from the four biggest counties in Estonia, and the two stage sampling technique was implemented: random selection of schools (urban vs rural schools, and Estonian vs Russian speaking schools); and a random selection of single sixth grade classes per school. The sample of the present study included 903 students from 52 schools with a mean age of 12,8 (SD=0,4) who answered the fire safety risk behaviour questionnaire. The sample was composed based on the proportions of sixth-grade students in Estonia, and the total sample included students representative by gender (50,1% of male), residency (81,1% from urban schools), and ethnicity (69% from Estonian speaking schools).

1.2 PROCEDURE

Most of the students filled in the fire safety questionnaire via the web-based LimeSurvey software, as an exception paper forms were also used in the classroom. Questions measuring fire related behaviour (dependent variables), independent variables, and the corresponding coding systems are described in Table 1. The students' fire safety questionnaire was developed by the scientists and experts of the University of Tartu and the Estonian Rescue Board based on previous studies (Kafry, 1980; Grolnick et al., 1990; Fessler, 2006; Morrongiello et al., 2008; Morrongiello, Zdzieborski & Normand, 2010). The questionnaires used in the Russian speaking schools were translated from Estonian into Russian. The questionnaires were administered in the classroom during a 45 min session. When they filled the questionnaire only a study assistant was in the classroom who explained the aim and procedure of the session and if needed answered students' questions. Unique codes were used instead of names on the questionnaires to ensure students' anonymity.

The research project was approved by the Research Ethics Committee of the University of Tartu.

1.3 DATA ANALYSIS

Students were divided into 3 risk groups (High-risk, Low-risk and No-play) based on their reported fire-play during the previous 12 months. The High-risk group includes children who declared playing with fire "very often" or "often". This group characterises children whose fire-play is usually intentional and malicious, including a wish to burn things. High frequency of fire-play can often lead to dangerous consequences (causing fire, getting injured, etc.). Children who reported playing with fire "sometimes" or "seldom" where classified to the Low-risk group. It describes children who usually have a low level of intent to inflict harm. Fire-play occurs mainly because of curiosity and awareness of matches. Despite the lower frequency the consequences of fire-play might still be dangerous. Children who have not declared playing with fire recently belong to the No-play group that is used as a reference group. (Kafry, 1980, p.2; Kolko, 2001, p.359; Putnam & Kirkpatrick, 2005, p.2; Fessler, 2006, p.436; Hall, 2010, p.6; Harpur, Boyce & McConnel, 2013, p.73)

Simple logistic regression analysis was used to assess how the individual and environmental variables predict belonging to the High-risk and Low-risk group compared to the No-play group. Results were provided as odds ratios and 95% confidence intervals. For statistical analyses, SPSS 20 software (IMB Statistics) was used. Values of $p<.05$ were considered statistically significant.

TABLE 1. Description of analysed measures.

Measure	Description of measures / examples
BEHAVIOUR	
Belonging to the risk-group	"Have you played with matches, lighters or any other source of ignition during the last 12 months?" Responses to the 5-point frequency scale – „very often" to „no play" – were categorised into three groups: 1) High-risk group – "very often" and "often"; 2) Low-risk group – "sometimes" and "seldom"; 3) No-play group – "not played".
PERSONAL FACTORS	
Socio-demographic background	Gender – male/female. Ethnicity (based on the language of school) – Estonian/ Russian. Residency – urban/rural. Family (living together with 2 parents, single parent, or living separately from parents most of the days during the week). Type of heating: fireplace or stove at home (yes/no).
Knowledge and skills	
Knowledge of fire risk	We asked 8 questions about the risk of fire, spread of fire, and the health risks; with multiple-choice answers with one right answer. We standardised the right answers to describe the level of knowledge on a 100 point scale. e.g., "What is the biggest risk to health during a fire?"
Knowledge of right behaviour during fire	We asked 4 questions about the right behaviour during a fire; with multiple-choice and yes/no answers. Every question had only one right answer. We standardised the right answers to describe the level of knowledge on a 100 point scale. e.g., "Which is the safest mode to leave the room during a fire?"
Self-estimated skills of safety	We evaluated the children's self-estimation of their skills: 1) using a fire extinguisher, and 2) making a campfire. (yes or no)
Self-reported behaviour during fire	We asked about children's behaviour in case of a fire at home with 4 answers. First, we compared the highest-level risk behaviour ("I will definitely start to extinguish the fire") with the other answers (classified as yes vs no). Secondly, we compared the safest behaviour ("I will leave the house immediately and call for help") with the other answers (classified as yes vs no).

TABLE 1. Continued

Direct personal experience with fire	
Personal negative experience of a fire accident	We asked about 3 opportunities of previous negative experience – fire accident at home, child caused a fire, or someone close has been injured or died in a fire accident. If any of these questions was answered "yes", we labelled the person as "experienced".
Personal experience with the use of fire	Four items were used to measure if and how children got personal experience in using fire in last 12 months: 1) heating the oven, 2) making a campfire, 3) burning a candle, 4) smoking. We evaluated separately each of these experiences, (yes or no).
FACTORS OF SOCIAL ENVIRONMENT	
Observational learning	
Parents' related safety behaviour at home and the role and example of parents	Four items were used: 1) was a smoke detector installed (yes or no); 2) was the smoke detector tested and maintained (yes or no); 3) if there is a smoker in the household (yes or no); 4) who heats the oven or fireplace (children or only adults).
Personal role models	The children were asked who do they set as an example of fire safety with multiple-choices (e.g. mother, father, friend, celebrity or media-stars), (yes or no for each choice).
Verbal persuasion	
Source of warning about fire dangers?	We asked who has warned about fire dangers. The question was with multiple choices (e.g. mother, father, and friends), (yes or no for each choice).
Source of fire safety information and knowledge	Where have they got their knowledge of fire safety? Multiple choices (e.g. friends, parents, internet, fire service, etc), (yes or no for each choice).
Fire safety activities at school	E.g. participating in the safety camp, (yes or no).
Expectations for fire safety activities at school	We asked the students to evaluate opportunities of how school can help to raise children's safe behaviour (e.g. if the safety issues should be cross-curricular topics). We also asked if children are interested in learning to make a campfire or to use a fire extinguisher, (yes or no).

RESULTS

We analysed fire-play based on different levels of risk – High-risk and Low-risk versus No-play. The distribution of children by risk of fire-play (Table 2) revealed that 54.8% of the sample reported playing with fire during the last 12 months. We expect that for the children of the Low-risk group the main motives for fire starting might be fun and curiosity, and their fire-play depends much on the involvement with and/or awareness of fire as supposed by Kolko (2001, p.359) and Fessler (2006, p.436). Children from the High-risk group have reported playing with fire often or very often and we suppose that this is a possible warning of risk behaviour that is far beyond normal curiosity.

TABLE 2. Children's distribution by the risk groups of fire-play.

Risk group	N	%
High-risk	134	14.8
Low-risk	361	40.0
No-play	408	45.2

TABLE 3. Personal factors predicting the risk of playing with fire.

Socio-demographic predictors	High-risk vs No-play OR (95% CI)	Low-risk vs No-play OR (95% CI)
Gender: male vs female	**2.81 (1.87-4.22)**	**1.78 (1.34-2.37)**
Ethnicity: Estonian vs Russian	1.055 (.698-1,594)	**1.57 (1.15-2.14)**
Residency: urban vs rural area	.74 (.46-1.21)	.80 (.55-1.14)
Family: living without parents vs 2 parents	**4.89 (1.52-15.80)**	1.67 (.52-1.64)
Family: single parent vs 2 parents	1.40 (.87-2.25)	1.15 (.81-1.64)
Type of heating: fireplace or stove at home (yes vs no)	.91 (.61-1.35)	**1.34 (1.01-1.78)**
Knowledge and skills		
Knowledge of fire risk	**.79 (.70-.90)**	.93 (.85-1.03)
Knowledge of right behaviour during fire	**.69 (.57-.85)**	1.00 (.84-1.18)

TABLE 3. Continued

Self-reported dangerous behaviour: „In case of fire I will definitely start to extinguish the fire" (yes vs no)	**2.21 (1.35-3.62)**	1.03 (.67-1.57)
Self-reported safe behaviour: „ In case of fire I will leave the house immediately and call for help" (yes vs no)	**.37 (.24-.56)**	**.74 (.55-1.00)**
I can make a campfire (yes vs no)	**3,60 (2.21-5.84)**	**2.29 (1.69-3.11)**
I can use a fire extinguisher (yes vs no)	**1.97 (1.32-2,939)**	**1.43 (1.07-1.90)**

Direct personal experiences with fire		
Personal negative experience with a fire accident (yes vs no)	**3,29 (2.14-5.06.)**	**1.72 (1.22-2.43)**
I have made a campfire (yes vs no)	**11.98 (7.06-20.33)**	**4.20 (3.10-5.70)**
I have smoked (yes vs no)	**8.94 (5.60-14.30)**	**4.31 (3.06-6.09)**
I have heated an oven (yes vs no)	**5.44 (3.47-8.52)**	**2.82 (2.10-3.79)**
I have burned a candle (yes vs no)	**4.84 (2.52-9.30)**	**4.56 (3.00-6.94)**

Values p<.05 are marked in Bold.

Table 3 gives an overview of the main differences of personal factors that describe (portrait) the risk groups. The results show two significant demographic variables that predict belonging to the High-risk group: family structure and gender. Among socio-demographic variables, the strongest predictor of high-risk behaviour is children living without parents. We did not find living with a single parent to be a significant predictor of children's high-risk behaviour. There are also a significant number of gender related differences in playing with fire. Being a boy is a significant predictor of belonging to the High-risk group and to the Low-risk group compared to the No-play group. We also concluded that it is more likely to belong to the Low-risk group for Estonians and children from homes with a fireplace or stove compared to the No-play group. Still, these factors did not predict of belonging to the High-risk group. There was no significant difference in playing with fire between children living in urban or rural areas.

Analysis shows that previous personal experience with fire-incidents at home or among peers predicts children's higher fire-related risk

behaviour. There are significant differences between risk groups in experiences of using fire sources during the last 12 months. Children from the High-risk group have a lot of practice in outdoor activities like making a campfire and smoking compared to the No-play group. When comparing the indoor activities (heating the oven and burning a candle) we see a lower impact, but still strong significant differences between the High-risk and No-play groups. Children's experiences with the use of fire strongly predict their higher activity in playing with fire and therefore belonging to the High-risk group; especially when we evaluate their outdoor risk behaviour.

Children in the High-risk group have a lower knowledge of the risks of fire and safe behaviour during a fire. Their declared behaviour during a fire differs dangerously from the children from the No-play group. It is more likely that in case of fire they start to extinguish the fire by themself and less likely that they are going to evacuate from the building and call the emergency services than the No-play group. Children from the higher risk groups tend to underestimate the risk of fire and overestimate their own capabilities of action that might lead them to dangerous and risky behaviour.

TABLE 4. Factors of social environment predicting the risk of playing with fire

Observational learning	High-risk vs No-play OR (95% CI)	Low-risk vs No-play OR (95% CI)
Children are heating the oven (children vs only adults)	**2.55 (1.41-4.60)**	1.39 (.93-2.09)
Having a smoke detector at home (no vs yes)	**2.17 (1.27-3.71)**	**1.66 (1.09-2.55)**
Family member smokes (yes vs no)	**1.71 (1.10-2.67)**	**1.49 (1.10-2.03)**
Smoke detectors checked (no vs yes)	1.38 (.93-2.05)	**1.46 (1.10-1.94)**
Mother is a role model (yes vs no)	**.42 (.27-.66)**	.90 (.63-1.30)
Father is a role model (yes vs no)	.67 (.44-1.01)	1.23 (.89-1.68)
Friend is a role model (yes vs no)	**1.60 (1.03-2.50)**	**1.61 (1.16-2.24)**
Celebrity or media-star is a role model (yes vs no)	**2.61 (1.22-5.58)**	**1.96 (1.04-3.70)**
Verbal persuasion		
Mother has warned of dangers (yes vs no)	**.43 (.26-.71)**	1.00 (.64-1.55)

TABLE 4. Continues

Father has warned of dangers (yes vs no)	**.62 (.41-.94)**	1.43 (1.01-2.01)
Friend has warned of dangers (yes vs no)	**2.16 (1.39-3.34)**	**1.87 (1.34-2.61)**
I have learned from parents (yes vs no)	**.23 (.12-.45)**	**.53 (.29-.95)**
I have learned from teaching materials (yes vs no)	**.49 (.30-.80)**	1.19 (.79-1.79)
I have learned from fire and rescue authorities (yes vs no)	.93 (.55-1.59)	1.41 (.95-2.11)
I have learned from a class teacher (yes vs no)	**.58 (.36-.93)**	.85 (.58.-1.22)
I have learned from the internet (yes vs no)	.99 (.62-1,60)	1.14 (.81-1,59)
I have learned from friends (yes vs no)	**2.33 (1.54-3.54)**	**1.38 (1.03-1.85)**
I have learned from safety camp (yes vs no)	1.38 (.89-2.15)	1.05 (.76-1.44)
I have shared the new knowledge from school with parents (yes vs no)	.93 (.61-1.42)	.91 (.67-1.23)
I have participated in the *„Kaitse end ja aita teist"* ("Protect Yourself and Help Others") safety programm (yes vs no)	**1.83 (1.20-2.81)**	1.31 (.95-1.81)
Dealing with fire safety issues at school in the last 12 months (yes vs no)	**.69 (.57-.83)**	.88 (.77-1.01)
Expectations for fire safety activities at school		
Teachers should involve the safety issues as cross-curricular topics (yes vs no)	.89 (.59-1.34)	1.15. (.86-1.54)
Planning regular fire drills (yes vs no)	**.51 (.33-.79)**	1.21 (.84-1.74)
Participation in the activities of the rescue service (i.e. visiting fire station; public fire safety day) (yes vs no)	**.65 (.43-.97)**	.81 (.60-1.08)
I wish to learn about making a campfire (yes vs no)	**.62 (.42-.93)**	1.03 (.77-1.37)
I want to learn to use a fire extinguisher (yes vs no)	**.49 (.33-.73)**	**.74 (.55-.99)**

Values p<.05 are marked in Bold.

Table 4 provides an overview of the factors of social environment that characterise most of the differences in children's fire-related behaviour during the social learning process. When evaluating the role and example of parent's safety behaviour, especially the role of the mother, we can see this is a significant predictor of children's fire-related risk behaviour. Nevertheless, it can be seen that in the High-risk group, parents are not

as important role models as in the No-play group. The analyses show that children from homes where the children heat the oven instead of the parents, homes without a smoke detector, and homes where at least one of the parents smokes – are more likely to belong to the High-risk group compared to the No-play group. Missing smoke detectors and parent's smoking also predicts belonging to the Low-risk group compared to the No-play group. The results demonstrate that parents' unsafe behaviour is a significant predictor of children's fire-related risk behaviour that can lead to serious consequences.

Students from the High- and Low-risk group have higher odds of the influence and example of celebrities and friends compared to the No-play group. At the same time, only the High-risk group has declared lower odds of the influence of grown-ups – especially the mother. We can point out the important role of the mother as an influence and example in safety behaviour. We can conclude that students who do not see parents as examples, but at the same time take celebrities and friends as influencers show higher odds of fire-related risk behaviour.

There are a number of statistically significant differences between risk groups in the area of verbal persuasion. The analysis shows that students whose mother's and father's role in warning against dangers is low, have higher odds of high-risk fire-related behaviour. When analysing the parents' role in teaching, it revealed that students who have declared the lowest level of learning from parents have significant odds of belonging to the High-risk group. They are also the ones who have got less knowledge from the learning materials and from the class teacher compared to the No-play group. At the same time they have stated getting warned against dangers and learning safety issues from their friends that let us conclude that declaring learning from friends is a predictor of belonging to the High-risk group. But as High-risk students report more that they are involved in the "*Kaitse end ja aita teist*" ("Protect Yourself and Help Others") safety program at school this led us to believe that they like and remember these activities more than the No-play group.

Besides the differences, it is also important to find out the receptivity sources of knowledge where risk groups do not differ. Analysis revealed that getting knowledge from the fire authorities and from the internet does not give higher odds of belonging to any risk groups. We also see

that students from all risk groups are aware of sharing the knowledge from school with their parents.

Analysing the students' expectations for fire safety activities at school reveals that lower interest to take part in fire drills and fire service activities predicts belonging to the High-risk group. An interesting finding is that lower interest to learn practically making a campfire and using a fire extinguisher shows higher odds of belonging to the High-risk group. Students of different risk groups do not differ by the statement that teachers should involve safety issues as cross-curricular topics.

3. DISCUSSION

Based on our study we can emphasize the high prevalence of fire play among the young people. More than half of the 12 years old children of our study have played with fire during the last year and almost one in seven of them belong to the High-risk group. According to the earlier studies, Kolko (2002, p.17) concluded that among the school-aged youth, as many as 45% of students in primary grades acknowledge having played with fire. Different earlier surveys have found that fire play typically peaks in late childhood or early adolescence (Fessler, 2006, p.429); and children at the age of 12 have reported the highest level of recent fire play (Grolnick et al., 1990, p.131). Dolan et al. (2011, p.391) pointed out that by the age of 10 years most children have reasonable knowledge of fire safety, and the problematic firesetting tends to develop in those who have been inadequately supervised and those with high levels of individual and family psychopathology. Therefore, we can point out that a high level of fire play is not a minor problem, but a high potential risk that needs to be managed, not only by limitations and restrictions, but also by smart teaching and prevention work at school together with families and members of the community. It is also important to consider the children from different risk groups when planning appropriate prevention activities. We conclude our suggestions in the next chapters.

3.1 PERSONAL FACTORS AND FIRE-RELATED RISK BEHAVIOUR

3.1.1 Socio-demographic predictors

Our study finds that gender is an important variable to explain socio-demographic differences of playing with fire. Boys play much more often with fire than girls. Surveys based on the fire statistics usually present the risk of fire-play as a "boys' problem" because 9 of 10 fires caused by playing were set by boys (Kafry, 1980, p.4; Ying & Ho, 2001, p.40; Dadds & Fraser, 2006, pp.584-585; Evarts, 2011, p.7). An interesting finding in the present study is that the gender difference is smaller when comparing the rare fire-play (mainly playing because of curiosity), but much bigger when children play with fire often. Morrongiello (1996, p.499) concluded

that in comparison to girls, boys reported more injuries and close calls, were more likely to repeat behaviours that had resulted in prior injuries, and were less likely to tell their parents about the events. One of the reasons for this is that parents socialise boys and girls differently regarding risk taking (Morrongiello, Zdzieborski & Normand, 2010, p.328). Thus we can conclude that in the teaching process it is important to pay equal attention to both – boys and girls – when preventing the risks of fire-play and pay extra attention to reduce the boys' risk of fire-setting behaviour.

Our study shows that the most important socio-demographic predictor of children's' high-risk behaviour was related to the structure of the family. Children living without both of their parents were most likely to show high-risk fire-related behaviour. Family-related predictors of children's problematic fire-setting behaviour have usually been associated with deprivation, unstable family units, and family psychopathology that is very often a reason for inadequate supervision (Harpur, Boyce & McConnel, 2013, p.77; Dolan et al., 2011, p.391). It can also lead to the lack of teaching safety issues at home and missing parental role models for safety. Although, many previous surveys and reviews (Kafry, 1980, p.9; Kendrick et al., 2010, p.3; Edelman, 2007, p.963; Dolan et al., 2011, p.387; Jennings, 2013, p.4) have pointed out the higher risk of injury in children from single parent and step parent families than those from two (natural) parent families, we did not find a statistically significant difference in risk behaviour between children from single parent and two parent families. Further research is needed to find out if the bigger everyday mobility in society and less time spent with the family have reduced the differences of parental support between families with both parents and a single parent. Children who are living together with both parents have much lower risk behaviour compared to ones who are living separately from parents most of the days during the week. Schools together with the community should pay extra attention to support, teach, and include the children who are living in dormitories, orphanages, or other places without parents.

The study concludes an interesting finding related to the role of the fireplace at home to children's fire-play. It has a statistically significant relation of belonging to the Low-risk group, but not to the High-risk group compared to the No-play group. Although the availability of sources of ignition was found to be a significant predictor of fire-play in many

studies (Grolnick et al., 1990; Towner & Warda, 1998, p.20; Harpur, Boyce & McConnel, 2013, p.79), we found that for the age-group 10-13 it is not the main reason. We find that the availability of sources of ignition enables the interest in fire-play, but it does not have an impact for high-risk fire-setting behaviour. Dietrich (1952, p.851) has analysed the efficacy of protective devices and educational efforts and emphasizes that these must be appropriate for the child's age, sex, developmental achievements, and opportunities. Hiding the sources of ignition is an important prevention measure for avoiding playing with fire because of curiosity among young children, but is not enough to prevent the fire-setting behaviour in the age group 10-13. High-risk fire related behaviour is not caused by the availability of sources of ignition, but still supports it.

3.1.2 Knowledge and skills

The current study shows that lower knowledge about the risk of fire and about safe behaviour during fire predicts higher fire-setting behaviour during early adolescence. Children who belong to the High-risk group had lower knowledge in most of the important fire safety issues (e.g. health risks, speed of fire spread, threats of using fire, fire safety requirements; evacuation, etc.) compared to the No-play group. The relationship between knowledge and risk-taking behaviour shows controversial results in the different studies. Grolnick et al. (1990, p.134) found that understanding the destructiveness of fire was unrelated to fire play. It is also concluded that better safety knowledge does not play a role in risk-taking behaviour (Schieber & Vegega, 2002; Zeedyk et al., 2001). Fessler (2006) discussed that knowledge regarding institutionally-conveyed fire safety practices had no relationship with the extent of fire play because the principal motives for fire starting are "just for fun", "to see what would happen", "to destroy something", and "boredom". On the opposite side, Kolko (2001, p.359) declared that limited fire competence supports fire-play, that is consistent to our study.

Children's lower understanding of the risks of fire leads to more frequent and dangerous fire-play; and they would also more likely choose the more dangerous behaviour and make a wrong decision if they have to choose between extinguishing a fire or evacuating the room. The results

of our study showed that the High-risk group were more likely to start to extinguish the fire and less likely to evacuate from the building than the No-play group. Several authors underline that overestimation of their physical abilities and perception of control over dangerous situations are positively related to fire play and are the reasons for making errors (Grolnick et al., 1990, p.134; Schwebel & Plumert, 1999, p.702). We also found that children who reported high or low level fire-play estimate their skills of making a fire and using a fire-extinguisher much higher than children of the No-play group.

Present findings indicate that high-risk behaviour is related to lower knowledge. Therefore, it is important to focus on educating the children from the High-risk group by teaching them safety issues. Teaching fire safety at school should take this into account and use suitable methods when teaching children who underestimate the risk of fire and overestimate their own skills. It is very important that teaching fire related topics is focused on safety behaviour. Especially when teaching children from the High-risk group who have a higher, but often inadequate perception of their skills. For example, when teaching the use of a fire extinguisher it is extremely important to teach in which conditions it is safe enough to use an extinguisher during a fire. We admit that narrow factual based knowledge is not enough to reduce risk behaviour and agree with Morrogiello (2008, p.178) that interventions need to include promoting positive attitudes towards safe behaviour. We also emphasize that teaching should be appropriate to the age of the children.

3.1.3 Learning by direct personal experiences

In our study, we analysed the associations of negative and positive experiences of fire-play. The current study shows that students who have had previous negative experiences with fire (fire at home, caused fire by themself, etc) still have declared higher fire-play during the last 12 months. We can deduce from this that earlier negative experiences do not have enough impact to reduce the interest in fire-play. Kafry (1980, p.11) also realised that accidents in the children's past are one of the frequent problems that is common for children who have often played with fire. Morrongiello et al. (2008, p.178) have similar findings that children

who have had more prior injury experiences are more likely to report risky practices, hence, they do not learn risk avoidance from injury experiences. This result does not support the conclusion of Cole et al. (2006) who found that 9 out of 10 children who have started a fire never started another once they see the consequences of their actions. Morrongiello et al. (2008) has explained that experiencing a serious injury does not deter children from avoiding the risk behaviour that led to injury because they are attributing injury to bad luck, as opposed to their own behaviour, or their attitudes towards safety rules. This finding suggests expanding child-directed injury prevention interventions to focus more on attitudes (Morrongiello et al., 2008, 179).

We compared the students' exposure to different kinds of fire-related activities and found that the more experience they have the more frequently they have also declared playing with fire. We found that making a campfire, smoking, heating the stove, and burning candles are important predictors of frequent fire play. It confirms the idea that the more practice a child has with fire, the more competent and falsely "in control" he or she may feel, which is likely to increase the behaviour rather than extinguish it (Grolnick et al., 1990). The earlier a child gets the "positive" experiences the harder it is to convince them about the danger of fire and change their risky behaviour. Kolko (2002, pp.19-20) claims that it is quite impossible to convince even a 4-years-old child about the danger of playing with fire if a child has played with fire a few times, and nothing bad happened. The importance of learning by personal experiences is one of the cornerstones of Social Learning Theory. It is stated that the practical implementation of a new skill is more likely to lead to a lasting change in behaviour than written or oral persuasion or exemplary action by others (Farquhar et al., 1991, p.333).

Our findings confirm that children who have got successful experiences (rewarding) with the use of fire are estimating their skills high and tend to play with fire more often. At the same time, we got controversial results to the expected impact of the negative experiences. Despite their negative or unsuccessful experiences (punishing consequences) with fire, children still reported a high level of skills and higher frequency of fire-play. Social learning theory explains that one way how the behaviour can be shaped is by rewarding and punishing consequences (Bandura, 1971, p.5). Performance accomplishment as a source of efficacy information is

especially influencial: successes raise mastery expectations, but repeated failures lower them, particularly if mishaps occur early in the course of the event (Bandura, 1977, p.195). We can conclude that negative experiences are surprisingly not as good to shape the safety experiences as we expected. We therefore recommend paying more attention to children who have been exposed to fire incidents.

Prevention should focus on the interventions that help to avoid children's trial-and-error experiences in a dangerous way. It includes the parents' responsibility to keep matches away from children and teaching the safe use of fire related equipment. Trainings must provide practical, positive, and correct skills for safety. It is important to plan the interventions before they gain experiences on their own based on their age-appropriate interest. Children who have personal experience with fire without previous safety instruction should be taken as a special vulnerable risk group when planning fire safety prevention work. It is important that schools, families, communities, and relevant authorities are sharing information about the children at risk and plan the interventions in good cooperation.

3.2 FACTORS OF SOCIAL ENVIRONMENT

3.2.1 Observational Learning

The study shows that children whose family members smoke have a higher likelihood to belong to the High-risk group. Smoking has been shown as the most common risk factor associated with parents; 8 of the 9 fire starters (88%) had at least one parent/carer that smoked and, undeniably, incidents of fire-play were strongly influenced by parents' smoking habits - children attempted to copy the physical act of igniting objects. (Harpur, Boyce & McConnel, 2013, p.79). Children's attitudes to fire safety and safe behaviour depend a lot on the behaviour of adults. Important factors that predict children's high-risk behaviour are related with the parents' dangerous behaviour and unsafe home environment. Parents should be very aware of their own safe behaviour and be ready to teach them critical safety messages on a one-to-one basis (Kolko, 2002, p.20). Missing or regularly untested smoke detectors show

the carelessness and underestimation of home fire safety by parents. That shapes the attitudes and habits of children.

An interesting finding is that a significant predictor of high interest in playing with fire is the assignment of responsibilities at home - that parents are having their children heat the oven or fireplace themselves. In these homes, the children's use of fire is accepted and matches or lighters are more easily accessible. We might presume that these children have acquired the experience of using matches with practical purposes, so they do not have an interest to play with matches at all, but the study showed the opposite. Children who have used the fire in the special safe place might perceive the dangers inadequately and based on positive experiences play more with fire.

When analysing the place of previous experiences of the High-risk group with the use of fire we can see the predominance of outside fire-related activities (making a campfire and smoking). Dougherty et al. (2007, p.473) compared the age groups 6-10 and 11-17 and found that fire-play outside the home increases for older students. An important difference between these age groups is the motivation behind fire-play. For the younger children it is based on curiosity, while for the older age group the most common perceived motivations were peer-pressure and impulse control. Henderson & MacKay (2009, p.132) found that 79% of the children who have engaged in fire-starting had fire-related episodes involving participation with other children. We can conclude that peer-pressure is an important variable for the High-risk group at the age of 12, but it does not have an extra impact for playing with fire because of curiosity. At this age the decrease of parental supervision and increase of peer-pressure are having an important impact on the risk behaviour. Morrongiello et al. (2008, p.179) propose to target groups of friends, as opposed simply to individuals, when planning interventions that promote positive attitudes toward safety issues because of the increasing importance of peer opinion in teenagers.

We found that children's risk behaviour depends a lot on their social relations inside and outside the family. Children who declared lower trust of their parents and higher trust to celebrities and friends as an example of their safety behaviour have a higher likelihood to belong to the High-risk group. It also means that children from the High-risk

group are less reachable through their parents. That states a challenge for schools, rescue services, and the community to influence these children's attitudes to trust and learn safety issues at school. We can conclude that parents' unsafe behaviour is a significant predictor of children's high fire-related risk behaviour because of the failed results of observational learning. Considering the importance of observational learning in children's risk behaviour, it is necessary to teach parents, and emphasize the importance of their position as role models in fire-safe behaviour. Interventions aimed at children need to take into account the child's social relationships in order to find out who may have the greatest influence on their behaviour. To change the attitudes toward safe behaviour of teens it is useful to organise attractive courses to the groups of friends or youth in the environment that interests them. Celebrities and influencers can also be used to support the spread of safety attitudes.

3.2.2 Verbal persuasion and expectations for schools

The study shows that children from the High-risk group tend to evaluate the role of education and verbal persuasion low to get new knowledge and skills. At the same time, they declared more personal experiences with fire, and we also conclude that they have not had a good social environment to get positive vicarious experiences. These findings confirm the previous conclusions that verbal persuasion is less powerful than performance accomplishment or vicarious experience (Rosenstock, Strecher & Becker, 1988, p.180; Bandura, 1977, p.198; Bandura, 1971, p.3). Based on the findings described in the previous chapters we claim that the main reason for the inefficiency of teaching is that many target groups are reached too late and the previous social learning process has already created inadequate knowledge, which is an unsuitable ground for new knowledge and retraining. Towner (1995, p.58) has emphasized that the challenge is to make the educational process more effective in all contexts in which it takes place and guarantee that it suits the target group.

We found significant differences between risk groups when they described their sources of fire safety knowledge. Children who belong to the High-risk group have declared a significantly lower role of parents in the teaching process than the No-play group. These children declare

getting knowledge from their friends. Missing the role of parents in the teaching process is one of the strongest predictors of children's fire-related risk behaviour. Boles et al. (2005, p.568) explained that children who reported less vulnerability to become injured at home were significantly more likely to engage in risky behaviour. That might be the direct consequence if the parents' role of warning children about the risks is insufficient. To decrease the number of children who belong to the High-risk group, it is important to increase the role of their parents to teach children, to behave as good examples, and guarantee the adequate parental supervision of children's safety behaviour. One of the opportunities is to use special fire safety courses for parents of the children from the High-risk group. Carroll et al. (1986) concluded that parental involvement in educational interventions has significantly increased the implementation of fire safety into the home. Harpur, Boyce & McConnel (2013) have also suggested that future prevention strategies should focus on reaching the parents of those deemed to be at risk. We propose that teachers development discussions with parents should have an important role in cooperation where they also discuss the child's possible risk behaviour and opportunities to work on the problem together.

Based on different studies Dougherty et al. (2007, p.475) have concluded that school-based programs can play an important part in the effort to reach not only the children in the classroom, but also their parents through discussion generated outside the classroom and take-home exercises that involve the parents. Our findings confirm this and surprisingly it revealed that although children from diferent risk groups evaluate the teaching at school very differently, we did not find significant differences between risk-groups to share the new knowledge from school with their parents.

Teaching safety issues to the children from the High-risk group is definitely challenging. Compared to the No-play group they have declared significantly lower interest in learning practical skills (e.g. making a campfire and the use of a fire extinguisher) or participating in regular fire drills and in different activities outside the school together with the rescue service. An interesting finding is that children from the High-risk group underestimate the role of teaching fire safety issues at school, but at the same time they have declared higher participation in the "*Kaitse end ja aita teist*" ("Protect Yourself and Help Others") course, which is a

more practical safety course. Based on this contradiction we propose to focus on practical skills when teaching safety issues at school and combine these with theoretical information that helps them better understand the risks in their everyday environment. Bandura (2004, p.158) also worried that educational efforts to promote health of youths usually produce weak results because they provide factual information and usually do little to equip children with the skills and efficacy beliefs. We conclude that despite the High-risk group's low interest in participating in educational programs, the usefulness of training practical skills at schools is promising. It is important that the main aim of teaching is to turn an interest in fire-setting to an interest in fire safety; and educational programs are tailored to the developmental level of the child and focused on the strategies for staying safe (Sharp et al., 2006, p.333; Kolko, 2002, p.26). Therefore, it is especially important to design very exciting hands-on trainings that will influence their skills and attitudes towards safe behaviour. To reach better to the most vulnerable children we also propose the wider use of schools' good practice to prefer sending children with higher risk behaviour to the safety camps.

Our study shows that the studied groups did not differ by the receptivity of learning fire safety issues from the internet, rescue authorities, fire camp, and subject teachers. There was also no difference between risk groups for the suggestion that teachers should involve safety issues as cross-curricular topics. Still, the High-risk group is less receptive to learning from a class teacher or learning from study materials by themselves, compared to the No-play group. It provides guidance on how to organise teaching so that children from different risk groups are equally interested and involved. The solution might be to use rescue service personnel together with teachers and teach it as cross-curricular topic at school. That kind of comprehensive approach where emergency service personnel, teachers, and community groups are combined has been proposed as an effective and successful method to teach fire safety skills (Dougherty et al., 2007, p.475; Sharp et al., 2006, p.334; Bandura, 2004, p.158; Warda, Tenenbein & Moffatt, 1999, p.224).

We can expect that school has an important role as a social balancer for children who have a deficit of knowledge and social support at home and belong to the high risk group. School has a challenge to fill the gaps of safety knowledge and change the children's attitudes to create them

equal opportunities and conditions for the future. That supports the idea that new school-based models of health promotion should operate together with the home, the community, and society at large (Bandura, 2004, p.158).

School also has an important role as an example of valuing safety culture. We have to bear in mind that children's homes and social relations are different; and it influences the children's safety attitudes through their lifespan. The primary role of school is to act as a role model when planning the safe environment for students, when organising fire evacuation drills, or when sharing the safety information. Schools should aim to be the ideal environment for children to feel safe, especially for the most vulnerable ones.

ACKNOWLEDGEMENT

This work was supported by the Health Promotion Research Programme and funded by the European Regional Development Fund under Grant TerVE, 3.2.1002.11-0002, the Estonian Research Council, and Institutional Research Funding under Grant IUT20-40.

DISCLOSURE STATEMENT

No potential conflicts of interest were reported by the authors.

Contacts:

Margo Klaos
University of Tartu, Institute of Social Studies, Tartu, Estonia
Estonian Rescue Board, Southern Rescue Centre, Tartu, Estonia
E-mail: margo.klaos@eesti.ee
Phone: +503 5112

Diva Eensoo
University of Tartu, Department of Family Medicine and Public Health, Tartu, Estonia
E-mail: diva.eensoo@ut.ee

Kadi Luht-Kallas
University of Tartu, Department of Education, Tartu, Estonia
Estonian Academy of Security Sciences, Rescue College, Tallinn, Estonia
E-mail: kadi.luht-kallas@sisekaitse.ee

Jaanika Piksööt
National Institute for Health Development, Tallinn, Estonia
E-mail: jaanika.piksoot@tai.ee

REFERENCES AND SOURCES

Bandura, A. (1971) *Social Learning Theory*. New York: General Learning Press.

Bandura, A. (1977) Self-efficacy: Toward a Unifying Theory of Behavioral Change. *Psychological Review*. 84 (2). pp 191-215.

Bandura, A. (1989) Social Cognitive Theory. In Vasta, R. (ed.). *Annals of child development. Vol. 6. Six theories of child development*. Greenwich, CT: JAI Press, pp 1-60.

Bandura, A. (1998) Health promotion from the perspective of social cognitive theory. *Psychology and Health, 13*, pp 623-649.

Bandura, A. (2001) Social cognitive theory of mass communications. In Bryant, J. & Zillmann, D. (eds.). *Media effects: Advances in theory and research, 2.nd ed.* Hillsdale, NJ: Lawrence Erlbaum, pp 121-153.

Bandura, A. (2004) Health Promotion by Social Cognitive Means. *Health Education & Behavior*, 31, 143-164.

Boles, R.E., Roberts, M.C., Brown, K.J. & Mayes, S. (2005) Children's Risk Taking Behaviors: The Role of Child-Based Perceptions of Vulnerability and Temperament. *Journal of Pediatric Psychology, 30, 7,* pp562-570.

Braungart, M.M., Braungart, R.G. (2007) Applying learning theories to healthcare practice. In Bastable S.B., Gramet P., Jacobs & K., Sopczyk, D.L. (eds). *Health professional as educator. Principles of teaching and learning.* Jones & Bartlett Learning, pp 51-90.

Carroll, W., Augsten, W., Hansbrough, J. & Williams, S. (1986) The Development of a Program for Juvenile Fire Offenders. *The Journal of Burn Care & Rehabilitation, 7, 3,* pp 253-256.

Cole, R., Crandall, R., Kourofsky, C., Sharp, D., Blaakmann, S. & Cole, E. (2006) *Juvenile Firesetting: A Communitiy Guide to Prevention & Intervention.* Pittsford, New York: Fireproof Children/Prevention First.

Dadds, M.R. & Fraser, J.A. (2006) Fire interest, fire setting and psychopathology in Australian children: a normative study. *Australian and New Zealand Journal of Psychiatry, 40*, pp 581-586.

Dietrich, H.F. (1952) Clinical application of the theory of accident prevention in childhood. *American Journal of Public Health, vol 42*, pp 849-855.

Dolan, M., McEwan, T.E., Doley, R. & Fritzon, K. (2011) Risk factors and risk assessments in juvenile fire-setting. *Psychiatry, Psychology and Law, 18, 3,* pp 378-394.

Dougherty, J., Pucci, P., Hemmila, M.R., Wahl, W.L., Wang, S.C. & Arbabi, S. (2007) Survey of primary school educators regarding burn-risk behaviors and fire-safety education. *Burns, 33*, pp 472-476.

Edelman. L.S. (2007) Social and economic factors associated with the risk of burn injury. *Burns, 33,* pp 958-965.

Evarts, B. (2011) *Children playing with fire, 12/11.* NFPA Fire Analysis and Research, Quincy, MA.

Farquhar, J.W, Fortmann, S.P., Flora, J.A. & Maccoby, N. (1991) Methods of Communication to Influence Behaviour. In Holland, W.W., Detels, R. & Knox, G. (eds.). *Oxford Textbook of Public Health. Second edition. Volume 2. Methods of Public Health*. Oxford Medical Publications, pp 331 – 344.

Fessler, D.M.T. (2006) A Burning Desire: Steps Toward an Evolutionary Psychology of Fire Learning. *Journal of Cognition and Culture, 6.3-4,* pp 429-451.

Grolnick, W.S., Cole, R.E., Laurenitis, L. & Schwartzman, P. (1990) Playing With Fire: A Developmental Assessment of Children's Fire Understanding and Experience. *Journal of Clinical Child Psychology, 19, 2,* pp 128-135.

Grusec, J.E. (1992) Social Learning Theory and Developmental Psychology: The Legacies of Robert Sears and Albert Bandura. *Developmental Psychology, 28, 5.* Pp776-786.

Hall Jr., J.R. (2010) *Children playing with fire, 11/10.* NFPA Fire Analysis and Research, Quincy, MA.

Harpur, A.P., Boyce, K.E. & McConnell, N.C. (2013) An investigation into the circumstances surrounding fatal dwelling fires involving very young children. *Fire Safety Journal, 61,* pp72-82.

Henderson, J. & MacKay, S. (2009) Retail availability of fire-starting materials and their misuse by children and adolescents. *Fire Safety Journal, 44,* pp 131-134.

Istre, G.R., McCoy, M., Carlin, D.K. & McClain, J. (2002) Residential fire related deaths and injuries among children: fireplay, smoke alarms, and prevention. *Injury Prevention, 8,* pp 128-132.

Jennings, C.R. (2013) Social and economic characteristics as determinants of residential fire risk in urban neighborhoods: A review of the literature. *Fire Safety Journal, 62, A,* pp 13-19.

Kafry, D. (1980) *Fire-Play and Fire-Setting of Young Children*. US Department of Health, Education & Welfare, National Institute of Education.

Kendrick, D., Coupland, C., Mason-Jones, A.J., Mulvaney, C., Simpson, J., Smith, S., Sutton, A. & Watson, M (2010) Home safety education and provision of safety equipment for injury prevention (review). *Cochrane Database of Systematic Reviews, issue 7.*

Kolko, D.J. (2001) Efficacy of Cognitive-Behavioral Treatment and Fire Safety Education for Children Who Set Fires: Initial and Follow-up Outcomes. *J. Child Psychol. Psychiat, 42, 3,* pp 359-369.

Kolko, D.J. (ed.) (2002) *Handbook on Firesetting in Children and Youth*. San Diego: CA, Academic Press.

McAlister, A.L., Perry, C.L. & Parcel, G.S. (2008) How individuals, environment, and health behaviour interact. Social Cognitive Theory. In Glanz, K., Rimer, B.K.& Viswanath, K. (eds.). *Health behaviour and health education. Theory, research, and practice, 4th ed*. San Francisco: CA, Jossey-Bass, pp 169-188.

Morrongiello, B.A. (1996) Children's Perspectives on Injury and Close-Call Experiences: Sex Differences in Injury-Outcome Processes. *Journal of Pediatric Psychology, 22, 4,* pp 499-512.

Morrongiello, B.A., Cusimano, M., Orr, E., Barton, B., Chipman, M., Tyberg, J., Kulkarini, A., Khanlou, N., Masi, R. & Bekele, T. (2008) School-age children's safety attitudes, cognitions, knowledge, and injury experiences: how do these relate to their safety practices? *Injury Prevention, 14,* pp 176-179.

Morrongiello, B.A., Zdzieborski, D. & Normand, J. (2010) Understanding gender differences in children's risk taking and injury: A comparison of mothers' and fathers' reaction to sons and daughters misbehaving in ways that lead to injury. *Journal of Applied Developmental Psychology, 31,* pp 322-329.

Putnam, C.T. & Kirkpatrick, J.T. (2005) Juvenile Firesetting: A Research Overview. *Juvenile Justice Bulletin, May.* U.S. Department of Justice.

Roberts, I. & Power, C. (1996) Does the decline in child injury mortality vary by social class? A comparison of class specific mortality in 1981 and 1991. *BMJ, 313,* pp 784-786.

Rosenstock, J. M., Strecher, V. J. & Becker, M. H. (1988) Social Learning Theory and the Health Belief Model. *Health Education Quartely, 15(2)*, pp 175-183.

Schieber, R. & Vegega, M. (2002) Education versus environmental countermeasures. *Injury Prevention, 8,* pp 10-11.

Schwebel, D.C. & Plumert, J.M. (1999) Longitudinal and Concurrent Relations among Temperament, Ability Estimation, and Injury Proneness. *Child Development, 70, 3,* pp 700-712.

Sethi, D. et al. (2008) *European report on child injury prevention*. Copenhagen: World Health Organization Europe.

Shai, D. & Lupinacci, P. (2003) Fire Fatalities Among Children: An Analysis Across Philadelphia's Census Tracts. *Public Health Reports, 118*, pp 115-126.

Sharp, D.L., Blaakman, S.W., Cole, E.C. & Cole, R.E. (2006) Evidence-Based Multidisciplinary Strategies for Working With Children Who Set Fires. *Journal of the American Psychiatric Nurses Association, 11,* pp 329-337.

Zeedyk, M.S., Wallace, L., Carcay, B., Jones, K. & Larter, K. (2001) Children and road safety: increasing knowledge does not improve behaviour. *British Journal of Educational Psychology, 71 (4)*, pp 573-594.

Towner, E.M.L. (1995) The role of health education in childhood injury prevention. *Injury Prevention, 1,* pp 53-58.

Towner, E. & Warda, H. (1998) Prevention of injuries to children and young people: the way ahead for the UK. *Injury Prevention, 4*, pp 17-25.

Towner, E. & Scott, I. (2008) Child injuries in context. In Peden, M. et al. (eds.) *World report on child injury prevention*. Geneva: World Health Organization Press Publishing, pp 1-28.

Warda, L., Tenenbein, M. & Moffatt, M.E.K. (1999) House fire injury prevention update. Part II. A review of the effectiveness of prevention interventions. *Injury Prevention, 5,* pp 217-225.

Ying, S.Y. & Ho, W.S. (2001) Playing with fire – a significant cause of burn injury in children. *Burns, 27*, pp 39-41.

THE PLACE AND CONTENTS OF GOOD ADMINISTRATION IN ESTONIAN LAW ON THE EXAMPLE OF TERMINOLOGICAL DIVERSITY BASED ON CASE-LAW AND THE PRACTICE OF THE CHANCELLOR OF JUSTICE

Sille Allikmets, Magister iuris
Member of the Estonian Bar Association and an attorney-at-law at the Aavik & Partners Law Office

Keywords: good administration, terminology, Estonian law

INTRODUCTION

The term "*good administration*" is well-known in the laws of the European Union and Estonia. There is no ambiguity in the terminology of good administration with regard to the English approach in EU law, as *the right to good administration* is referred to *expressis verbis* and contained in Article 41 of the Charter of Fundamental Rights of the European Union proclaimed in Nice on the 7th of December 2000 (EU Charter of Fundamental Rights. OJ 2012/C 326/02). Pursuant to subsection 1 of the aforementioned, *the right to good administration* means that the institutions and bodies of the Union must handle one's affairs impartially, fairly and within reasonable time. These three principles can be called the key elements of good administration. Through their wording, the key elements of good administration allow the principle of good administration to provide a rather broad and varied content. To avoid this, Article 41 (2) of the Charter specifies the content of the key elements of good administration, providing everyone with the right to be heard before any individual measure which would affect him or her adversely is taken (EU Charter of Fundamental Rights. OJ 2012/C 326/02 Art 41 (2) (a)), to have access to his or her file (EU Charter of Fundamental Rights. OJ 2012/C 326/02 Art 41 (2) (b)), to demand reasons from the administration for its decisions (EU Charter of Fundamental Rights. OJ 2012/C 326/02 Art 41 (2) (c)), to determine the language to be used (EU Charter of Fundamental Rights. OJ 2012/C 326/02 Art 41 (4)) and to have the right to demand damages to be made good (EU Charter of Fundamental Rights. OJ 2012/C 326/02 Art 41 (3)). Through the regulation mentioned above, EU law has defined the term of *right to good administration* through specific content elements.

In Estonian law, only subsection 19 (1) of the Chancellor of Justice Act (Chancellor of Justice Act. RT I 1999, 29, 406) refers to good administration, more specifically, to good administrative practice, providing everyone the right of recourse to the Chancellor of Justice in order to have his or her rights protected by way of filing a petition to request verification whether or not a state agency, local government agency or body, legal person in public law, natural person or legal persons in private law performing public duties adheres to the principles of observance of the

fundamental rights and freedoms and good administrative practice. It is not clear in the context of the aforementioned provision nor other provisions of the same act as to which specific elements are included in the concept of *good administrative practice*.

According to the judicial practice of the Supreme Court (Judgement of the Constitutional Review Chamber of the Supreme Court of 17.02.2003, 3-4-1-1-03, Clause 16), the *right to good administration* is subordinated to section 14 (Section 14 of the Constitution: "It is the duty of the legislature, the executive, the judiciary, and of local authorities, to guarantee the rights and freedoms provided in the Constitution.") of the Constitution of the Republic of Estonia (The Constitution of the Republic of Estonia. RT 1992, 26, 349), according to which comments, the substantive protection sphere of the section includes the fundamental right to *good administration* as a right specifying the right to organisation and procedure in the field of administrative law (The Constitution of the Republic of Estonia. Annotated edition. Juura 2017, page 203). Consequently, the *right to good administration* should be clear and unambiguous in Estonian law as well – similarly to the Charter of Fundamental Rights referred to in the article above, and as the Court of Justice has stated, the *right to good administration* does not confer rights on individuals, as such, unless it is an expression of specific rights within the meaning of Article 41 of the Charter of Fundamental Rights of the European Union declared on the 7th of December, 2000 (Judgement of the Court of First Instance of 04.10.2006 T-193/04: Hansa-Martin Tillack vs Commission of the European Communities, Clause 127 and the judgement cited therein).

Unlike EU law, where good administration has been given the legal value of everyone's fundamental right by the Charter and as such the fundamental right is embedded with clearly defined content elements, Estonian law lacks the necessary specificity. References to good administration are primarily made in judicial practice by using the terms "*right to good administration*", "*principle of good administration*" and "*good administrative practice*" but also "*practice of good administration*" and "*the principle of good administrative practice*" (Tallinn Administrative Court judgement of 11.07.2008 in administrative matter No. 3-08-390; Tartu Administrative Court judgement of 17.11.2014 in administrative matter No. 3-13-2063, Clause 14; Judgement of the Criminal Chamber of the

Supreme Court of 12.10.2016, 3-1-1-65-16, Clause 21). This article examines the different applications of terms related to good administration in the Estonian judicial practice – both in case law and the practice of the Chancellor of Justice, who performs provisional supervisory activities and thereby protects the fundamental rights and freedoms of individuals – by identifying whether different terms are also incorporated with different component elements. The concept of good administration-related terminology leads to the more general question regarding the legal value of good administration in Estonian law – whether it is a fundamental right, a general principle of law or custom. The terminological clarity of good administration is the first step in ensuring the protection of a person's subjective rights in situations where there is a need to rely on good administration. In order to invoke such rights, it must beforehand be clear whether a reference to a specific good administration-related term also relates to its relevant content or to good administration in general.

As a reference to the different terms of good administration in Estonian law, Article 41 of the EU Charter of Fundamental Rights has been used, to which the Supreme Court referred to already in 2003, i.e. before Estonia became a member of the EU and before the Charter became legally binding to the Member States (The Charter became legally binding with the entry into force of the Lisbon Treaty on 1 December 2009 and currently has the same legal value as the EU Treaties). The usage of the Charter as an example has been justified by the Supreme Court with the fact that the Charter itself is based, "inter alia, on the constitutional traditions of the Member States of the European Union and on the principles of democracy and the rule of law. The principles of democracy and the rule of law also apply in Estonia" (Judgement of the Constitutional Review Chamber of the Supreme Court of 17.02.2003, 3-4-1-1-03, Clause 16). Following the example of Article 41 of the Charter, the Supreme Court has also listed one's right to have access to their files, right to be heard, right to be entitled to compensation for damages caused by administrative bodies and the administrative bodies' obligation to justify their decisions as components of good administration (Judgement of the Constitutional Review Chamber of the Supreme Court of 17.02.2003, 3-4-1-1-03, Clause 15). In this article, Article 41 of the Charter of Fundamental Rights is used as a reference only for the content elements of good administration and the scope of the Charter, which under Article 51 (1) of the Charter is addressed to the institutions and bodies of the Union with due regard

for the principle of subsidiarity and to the Member States only when they are implementing Union law, has been disregarded (Explanations on the Charter of Fundamental Rights. „Explanations on Article 51 - Scope". – ELT C 303, 14.12.2007, pp 17-35).

1. THE RIGHT TO GOOD ADMINISTRATION

A key element in the development of good administration-related judicial practice is the Supreme Court's judgement of 2003, which, based on Article 41 of the Charter of Fundamental Rights, recognised everyone's *right to good administration* and incorporated it in accordance with the Charter with one's right to have access to their files, right to be heard, right to be entitled to compensation for damages caused by administrative bodies and the administrative bodies' obligation to justify their decisions (Judgement of the Constitutional Review Chamber of the Supreme Court of 17.02.2003, 3-4-1-1-03, Clause 15). As mentioned above in this article, the Supreme Court relied on the Charter of Fundamental Rights despite the fact that the Charter was not legally binding for Estonia at the time. Transposed from the preamble to the Charter of Fundamental Rights, the Supreme Court incorporated good administration as part of democracy and the rule of law, as well as other general principles and legal values of European law, which, irrespective of the legal validity of the Charter, were valid in Estonia at the time of that decision.

While Article 41 of the Charter of Fundamental Rights and the judicial practice of the Court of Justice (Judgement of the Court of First Instance of 04.10.2006 T-193/04: Hansa-Martin Tillack vs Commission of the European Communities, Clause 127 and the judgement cited therein) implementing it provides exhaustive content for *good administration*, the Estonian judicial practice extends the bounds of the *right to good administration* to a greater extent when compared to the regulation set forth in the Charter, additionally incorporating the right to challenge the decision of the administrative body under such right (Judgement of the Constitutional Review Chamber of the Supreme Court of 20.10.2009, 3-4-1-14-09, Clause 44). Undoubtedly, the described right serves as an important right of defence, which, within the contents of good administration but without using that term *expressis verbis*, has been mentioned in the Council of Europe Committee of Ministers resolution (77) 31 of 1977 on the protection of the individual in relation to the acts of administrative authorities (Resolution 77 (31) of the Council of Europe, „On the Protection of the Individuals in Relation to the Acts of the Administrative Authorities") as a safeguard in administrative proceedings, in addition

to the right to be heard, the right to access information, the right to be assisted and represented and the administrative bodies' obligation to state reasons for their actions. The base for the adoption of this resolution, despite the differences between the Member States' administrative and judicial systems, was the broad consensus on the primary principles which should guide the administrative procedure in order to ensure the fairness in relationships between the individual and the administrative bodies (Resolution 77 (31) of the Council of Europe, „On the Protection of the Individuals in Relation to the Acts of the Administrative Authorities"). By approaching the *right to good administration* through the interpretation of section 14 of the Constitution as a specification of general organisational and procedural rights in the field of administrative law (The Constitution of the Republic of Estonia. Annotated edition. Juura 2017, p 203), this principle also applies to the right to challenge the decision of an administrative body – to ensure fairness in relationships between the individual and the administrative bodies.

In addition to the right to challenge a decision, the Estonian judicial practice refers to negligence of an administrative body and maladministration as a violation of the *right to good administration* (Tallinn Administrative Court judgement of 27.01.2011 in administrative matter No. 3-10-1919, Clause 4) Such an "indictment" of negligence of an administrative body could be qualified as a breach of the general duty of care of the administrative body, which Article 41 of the Charter of Fundamental Rights does not specifically mention in the context of good administration. From the aspect of the protection of the subjective rights of a person, the duty of care of an administrative body plays an important role in the proper conduct of administrative procedures.

Pursuant to the Supreme Court's decision of 2003 referred to in this article, the Chancellor of Justice of the Republic of Estonia also recognises *the right to good administration* as everyone's fundamental right arising from section 14 of the Constitution. Contrary to the Charter of Fundamental Rights and the judicial practice of the Supreme Court, the Chancellor of Justice, in addition to *the right to good administration*, embodies the obligation of the public authorities to "act in a humane manner", additionally emphasising that "public authorities must show due care in their dealings with a person, treat him/her as a subject and not as an object, and contribute in every way to the effective protection of his/her rights

and freedoms." (Overview of the activities of the Chancellor of Justice in 2008. Tallinn 2009, pp 11-12; Overview of the activities of the Chancellor of Justice in 2009. Tallinn 2010, pp 17-18; Overview of the activities of the Chancellor of Justice in 2010. Tallinn 2011, p 17). *The right to good administration* as enforced by the Chancellor of Justice could thus be summarised as a separate duty of care in addition to the requirement of due diligence expressed above.

The analysis of Estonian judicial practice suggests that the content elements of *the right to good administration* are largely similar to those stipulated in Article 41 of the Charter of Fundamental Rights, integrating into its composition everyone's right to have access to their files, right to be heard, right to be entitled to compensation for damages caused by administrative bodies and the administrative bodies' obligation to justify their decisions. Nonetheless, Estonian judicial practice nor the Chancellor of Justice do not utilise the *right to good administration* identically to the Charter. Thus, the Estonian judicial practice incorporates everyone's right to challenge the decisions of an administrative body and the requirement of due diligence and the so-called duty of care of an administrative body into the composition of *the right to good administration*. It is difficult to argue that these elements do not specify the general organisational and procedural rights within administrative law. Therefore, for the purpose of section 14 of the Constitution, the content components differing from the ones stipulated in the Charter can be considered as component elements of *the right to good administration* as well.

The Supreme Court has recognised the *right to good administration* as a fundamental right of everyone (Judgement of the Constitutional Review Chamber of the Supreme Court of 17.02.2003, 3-4-1-1-03, Clause 16). In order to invoke a fundamental right, it must be clear and understandable, both verbatim and in substance. The Estonian law of today lacks such clarity, which in turn calls into question the value of the fundamental *right to good administration* itself. The question of whether good administration is a specific fundamental right or a general principle of law developed by judicial practice has also been raised at the EU level. Wathelet, an Advocate General of the European Court of Justice has given his opinion on this question, emphasising, that the title of the Charter alone, and, moreover, the title and wording of Article 41

of the Charter put an end to the uncertainty as to whether the *right to good administration* is a fundamental right or a general principle of law. Wathelet explains that "this is the '*right to good administration*', a right which includes the right of every person to be heard before any individual measure which would affect him or her adversely is taken, the right of every person to have access to his or her file, the obligation of the administration to give reasons for its decisions" (Opinion of Advocate General Wathelet in court case Marchiani vs parliament, ECLI:EU:C:2016:22, C-566/14 P, Clause 37). Advocate General Wathelet's position is supported by the above-mentioned standpoint of the European Court of Justice, according to which the *right to good administration* does not confer rights on individuals as such unless it is an expression of specific rights within the meaning of Article 41 of the Charter of Fundamental Rights (Judgement of the Court of First Instance of 04.10.2006 T-193/04: Hansa-Martin Tillack vs Commission of the European Communities, Clause 127 and the judgement cited therein).

Taking into consideration the differences in legal regulation between the EU and Estonian law, certain doubts arise as to whether it is correct within Estonian law to consider the *right to good administration* as a fundamental right, relying on the *principle of good administration* used and embodied in Estonian judicial practice. The following analysis clarifies whether Estonian judicial practice uses the terms "*right to good administration*" and "*principle of good administration*" as synonyms, or whether there are substantive differences between the fundamental right and *principle of good administration*, and thus whether Estonian law includes a specific (fundamental) *right to good administration* or a more general principle of such.

2. THE PRINCIPLE OF GOOD ADMINISTRATION

Article 41 of the Charter of Fundamental Rights, as well as the composition of the *right to good administration* as embodied by the Estonian judicial practice, does not explicitly mention the obligation to include a person, through which the judicial practice incorporates the *principle of good administration* (Judgement of the Administrative Chamber of the Supreme Court of 11.12.2006, 3-3-1-61-06, Clause 20, Clause 23; Judgement of the Administrative Chamber of the Supreme Court of 11.10.2007, 3-3-1-37-07, Clause 9; Judgement of the Administrative Chamber of the Supreme Court of 18.11.2009, 3-3-1-44-09, Clause 14). Without explicitly mentioning the obligation to include a person to a proceeding within the composition of *the right to good administration*, this obligation can be considered as a part of this composition "by default", given that neither the right to be heard stipulated in the Charter nor the right to access one's personal data can be exercised without including that person in the proceedings. On the example of the obligation to include a person in a proceeding, such a conclusion enables the terms – *right to good administration* and *principle of good administration* – to be used in the Estonian judicial practice as synonyms.

In incorporating the *right to good administration* in accordance with Article 41 of the Charter of Fundamental Rights, the judicial practice also mentions the right to be heard (Judgement of the Administrative Chamber of the Supreme Court of 11.10.2007, 3-3-1-37-07, Clause 9, Judgement of the Administrative Chamber of the Supreme Court of 19.12.2006, 3-3-1-80-06, Clause 20, Tartu Circuit Court judgement of 25.05.2012 in administrative matter No. 3-10-2889/46, Clause 16; Tartu Administrative Court judgement of 15.03.2007 in administrative matter No. 3-06-2484) and the obligation to state reasons (Judgement of the Constitutional Review Chamber of the Supreme Court of 30.09.2009, 3-4-1-9-09, Clause 31; Tartu Administrative Court judgement of 18.09.2018 in administrative matter No. 3-17-2076, Clause 18) for administrative acts as a substantive element of the *principle of good administration*. The mutual overlap of these content elements leads to the conclusion that the terms *right to good administration* and *principle of good administration* can only be used synonymously.

In addition to the similar content elements referred to above, Estonian judicial practice – unlike the Charter of Fundamental Rights and the given contents of the *right to good administration* – refers to the administrative body's obligation to justify their actions not only as a component of the *principle of good administration* (Judgement of the Administrative Chamber of the Supreme Court of 11.12.2006, 3-3-1-61-06, Clause 20, Clause 23; Tartu Circuit Court judgement of 10.11.2015 No. 3-14-186, Clause 14, Clause 17; Tallinn Circuit Court judgement of 29.03.2010 in administrative matter No. 3-09-277, Clause 12), but also as a subcomponent alongside it (Tallinn Circuit Court judgement of 08.04.2014 in administrative matter No. 3-12-2196, Clause 12; Tartu Circuit Court judgement of 05.02.2008 in administrative matter No. 3-07-38). In the latter case, the Court has emphasised that "the administrative body's duty to ensure that, in conjunction with the principle of investigation, the obligation to justify their actions and the *principle of good administration*, the person's lack of knowledge of the need to provide certain information would not become a hindrance" (Tallinn Circuit Court judgement of 08.04.2014 in administrative matter No. 3-12-2196, Clause 12). There is no doubt that the requirement for an administrative body to justify their actions specifies general administrative and procedural rights in the field of administrative law and thus also complies with the principle of good administration. The different approach to the administrative body's obligation to justify its actions within or outside the *principle of good administration* demonstrates the lack of unequivocal clarity on the meaning of good administration in Estonian law.

Unlike the Charter of Fundamental Rights and the content elements of the *right to good administration* as embodied by Estonian judicial practice, the case-law further incorporates the contents of the *principle of good administration* with the administrative body's obligation to respond (Judgement of the Administrative Chamber of the Supreme Court of 18.11.2009, 3-3-1-44-09, Clause 14), to investigate facts, gather evidence, consider different options (Judgement of the Administrative Chamber of the Supreme Court of 11.10.2007, 3-3-1-37-07, Clause 9; Judgement of the Administrative Chamber of the Supreme Court of 18.11.2009, 3-3-1-44-09, Clause 14) and to make reasonable efforts to eliminate or reduce the possible adverse effects (Judgement of the Administrative Chamber of the Supreme Court of 16.12.2010, 3-3-1-83-10, Clause 17), moreover, with the person's right to demand the administrative body to consider an earlier promise made to him or her and the legitimate expectation

that may have arisen from it (Tartu Administrative Court judgement of 15.03.2007 in administrative matter No. 3-10-769, Clause 16), the administrative body's obligation to interpret contentious facts in favour of that person (Order of the Administrative Chamber of the Supreme Court of 22.09.2014, 3-3-1-59-14, Clause 14) and with each party's requirement of respectful cooperation (Tallinn Administrative Court judgement of 15.06.2017 in administrative matter No. 3-16-2636, Clause 13.2). In addition to the listed, rather specific content elements, the Chancellor of Justice has further embedded the *principle of good administration* with the administrative bodies' obligation to "generally behave in the most so-called citizen-friendly way" (Overview of the activities of the Chancellor of Justice in 2006. Tallinn 2007, p 181). Whether the principle of good administration incorporated with such a requirement actually specifies general administrative and procedural rights in the field of administrative law (The Constitution of the Republic of Estonia. Annotated edition. Juura 2017, p 203) remains unanswered. In addition to the requirement of citizen-friendly conduct, the Chancellor of Justice has also mentioned administrative bodies' requirements such as purposefulness, simplicity, speed, involvement and hearing, helpfulness and impartiality as substantive elements of *the principle of good administration* as a "blanket term" (Overview of the activities of the Chancellor of Justice in 2006, p 179). The aforementioned list recognises, in light of the above, both the general principle of good administration (impartiality) contained in the Charter of Fundamental Rights and the specific content elements (i.e. the obligation to be consulted and heard, as well as the speed, which the Charter calls "reasonable time"). The "requirement of helpfulness" mentioned by the Chancellor of Justice as an additional element of good administration could be subordinated to the aforementioned duty of care, while the requirement of "purposefulness" and "simplicity" could be included in the requirement of due diligence or considered as completely separate component elements.

Turning back to the terms of good administration analysed insofar, with the purpose to answer the main question of the article – whether the use of different good administration-related terms in Estonian law is random or are different terms incorporated with different component elements – a comparative of the content elements of the *right to good administration* and the *principle of good administration* so far discussed show that there are both overlaps and differences between the content elements of the

two different terms. For example, by treating an administrative body's obligation to hear a person's testimony or to justify its actions as both, a *right to good administration* and a *principle of good administration*, it is possible to deduct the random use of good administration-related terms on the given example alone, hence disregarding the legal distinction between "(fundamental) rights" and "principles of law".

Unlike fundamental rights that are governed and implemented by the law, the general principles of law exist in both, written and unwritten law. Most of such principles are found as unwritten law, which is why it has been said that the general principles of law are unwritten law that are not based on the Treaty establishing the European Community (the European Union), but on the legal orders of the Member States of the EU. The general principles of law are dogmatically collected ideas that are not rules of law, but create cohesion only when combined with many principles. The general principles of law are created and found by the (European) court (J. Laffranque. Co-existence of the Estonian Constitution and European Law. Juridica III/2003, p 182). U. Lõhmus, the former Chief Justice of the Supreme Court, has also described the general principles of European Union law in the most general form as unwritten law introduced by the Court of Justice of the EU to fill in the gaps left by the European Union legislature as a tool for interpretation and as a basis for judicial review (U. Lõhmus. Fundamental Rights and General Principles of EU Law: Functions, Scope and Range. Juridica IX/2011, p 651). As in Estonian law, the gaps left by the legislator in the regulation of good administration have been primarily filled by judicial practice (which is supported and to some extent supplemented by the practice of the Chancellor of Justice), it is appropriate to consider good administration primarily as a legal principle of Estonian law through the term "*principle of good administration*" referred to in this section.

In addition to the terms "law" and "principle", Estonian case law and the practice of the Chancellor of Justice also considers good administration as a "practice". The following analysis shows whether or not there are differences in the contents of *good administrative practice* and *practice of good administration* formed by the Estonian case law and the practice of the Chancellor of Justice, but as well as its legal value, as compared to the *right to good administration* and the *principle of good administration* discussed above.

3. PRACTICE OF GOOD ADMINISTRATION AND GOOD ADMINISTRATIVE PRACTICE

A good illustration of the terminological ambiguity in Estonian law regarding good administration is the court's assessment, according to which an administrative body did not act in accordance with *good administrative practice* nor the *principle of good administration* (Judgement of the Administrative Chamber of the Supreme Court of 18.10.2004, 3-3-1-37-04, Clause 8). By identifying the existence of misconduct on the part of the administrative body against two different requirements of good administration, one can conclude that the court distinguishes and substantiates the *principle of good administration* from that of the *practice of good administration*. It is applicable to expand on the substantial differences between the two good administration-related terms through the same exemplary court case, which discussed the altering of the use of the applicant's plot of land by the local authority through the establishment of a comprehensive plan 3 years after the sale of the plot to the applicant and with it, the assignment of the plot that corresponded to the applicant's interests. According to the applicant, the alteration of land use through the introduction of a new comprehensive plan violated his rights and interests. This position was also upheld by the higher court, finding inconsistencies in the earlier positions of the administrative authority and in the conduct, which misled the applicant. According to the court, such misleading acts of the administrative body breached both, "*the practice of good administration*" and "*the principle of good administration*". From the composition of the *principle of good administration* discussed above, it is possible to describe through the similar usage of the same term in the instance of the referred court case, with the intent to incorporate the person's right to demand the administrative body take into account an earlier promise made to him or her and the legitimate expectation which may have arisen from it (Judgement of the Administrative Chamber of the Supreme Court of 18.11.2009, 3-3-1-44-09, Clause 14). However, in order to identify what the court has intended to separately incorporate - the term "*practice of good administration*" - within the same court case, it would be appropriate to more generally clarify such a term, as well as the term of *good administrative practice* embodied by the Estonian case law and the practice of the Chancellor of Justice in general.

In the case of the term of *practice of good administration* (as well as *good administrative practice*), the Estonian courts and the Chancellor of Justice refer to the obligation to include a person in administrative proceedings (Overview of the activities of the Chancellor of Justice in 2014. Tallinn 2015, p 114) and thereby the obligation to hear a person's opinion (Judgement of the Administrative Chamber of the Supreme Court of 13.06.2003, 3-3-1-42-03, Clause 37; Judgement of the Administrative Chamber of the Supreme Court of 25.11.2003, 3-3-1-70-03, Clause 19; Tallinn Administrative Court judgement of 11.01.2006 in administrative matter No. 3-05-339, Clause 7; Tartu Administrative Court judgement of 22.09.2009 in administrative matter No. 3-09-220; Tartu Administrative Court judgement of 02.07.2013 in administrative matter No. 3-13-729, Clause 19). As a part of the composition of *good administrative practice*, the case law and the practice of the Chancellor of Justice further expand on the administrative bodies' obligation to conduct the proceedings within a reasonable time (Tallinn Administrative Court judgement of 28.12.2007 in administrative matter No. 3-07-912; Tartu Administrative Court judgement of 19.10.2011 in administrative matter No. 3-11-870; Tartu Circuit Court judgement of 15.10.2013 in administrative matter No. 3-12-1000, Clause 19; Tartu Administrative Court judgement of 03.06.2014 in administrative matter No. 3-14-203, Clause 21; Overview of the activities of the Chancellor of Justice in 2006. Tallinn 2007, p 152; Overview of the activities of the Chancellor of Justice in 2012. Tallinn 2013, p 35), to justify their decisions (Tartu Circuit Court judgement of 20.09.2013 in civil case No. 2-12-10337, Clause 3; Tallinn Administrative Court judgement of 23.05.2007 in administrative matter No. 3-07-315; Tallinn Administrative Court judgement of 17.11.2014 in administrative matter No. 3-14-50113, Clause 11) and to compensate damages incurred to the parties of the proceedings (Tartu Administrative Court judgement of 15.11.2012 in administrative matter No. 3-12-1000). All of the listed components of good administration are inherent in both, the Charter of Fundamental Rights and the *right to good administration* and the *principle of good administration* embodied by Estonian case law and the practice of the Chancellor of Justice as referred to above, thereby allowing, through these content components, to infer a random use of various terms of good administration in Estonian law either as a law, principle or custom.

In addition to overlapping content components, Estonian judicial practice and the practice of the Chancellor of Justice also embody the *practice of good administration* (also referred to by the court as *good administrative practice*) with the administrative bodies' obligation to inform (Overview of the activities of the Chancellor of Justice in 2004. Tallinn 2005, pp 68, 107, 144; Overview of the activities of the Chancellor of Justice in 2005. Tallinn 2006, p 358), emphasising that due to the principle of democracy and good administration, the authority must inform the public of more important decisions more intensively than required by the law (Order of the Administrative Chamber of the Supreme Court of 07.05.2003, 3-3-1-31-03, Clause 26). In doing so, the court extends the scope of good administration beyond the boundaries of law. This position is also supported by the court's standpoint, according to which the procedural requirements set out in the Administrative Procedure Act must be regarded as minimum standards of *good administrative practice* (Tartu Administrative Court judgement of 22.12.2006 in administrative matter No. 3-06-2129), further taking account that *good administrative practice* additionally encompasses moral and ethical values (Tallinn Administrative Court judgement of 08.02.2008 in administrative matter No. 3-07-1178, Clause 33), as well as the duty of dignity, helpfulness and care of an official in accordance with the principle that the state must act in the best interests of the people (Tartu Administrative Court judgement of 14.11.2016 in administrative matter No. 3-16-1315, Clause 13). The Chancellor of Justice has also embodied the practice of good administration with similar values in mind, treating the violent and rude behaviour of an official as a breach of good administrative practice (Overview of the activities of the Chancellor of Justice in 2012, p 35).

In addition to addressing the individual content elements, the Chancellor of Justice has addressed the location and general nature of good administrative practice in various variations. Thus, through its competence, the Chancellor of Justice has defined the ability to respond to actions that are not in accordance with the "rule of law, the Constitution, laws or other legal instruments, or the *practice of good administration*" (Overview of the activities of the Chancellor of Justice in 2003-2004, p 44), placing the *practice of good administration* alongside the rule of law, the Constitution and other laws; at the same time, also respecting the *practice of good administration* as both a fundamental right (Overview of the activities of the Chancellor of Justice in 2004 p 196) and a constitutional principle

aimed at ensuring that administrative authorities are informed in adopting their decision, compelling the authorities to take into account a person's interests and improving the general quality of administrative decisions (Overview of the activities of the Chancellor of Justice in 2012 p 35). In addition to the varying definition of the legal position of (*the practice of) good administration*, some ambiguity can also be noted about the general nature of the good administration given by the Chancellor of Justice. More precisely, in addition to the right specifying the general organisational and procedural rights in the area of administrative law arising from the meaning of section 14 of the Constitution (The Constitution of the Republic of Estonia. Annotated edition. Juura 2017, p 203), the Chancellor of Justice has characterised good administrative practice as an unambiguous set of rules, which should nevertheless be a "perceptible code of conduct in dealing with people" (Overview of the activities of the Chancellor of Justice in 2005 p 252), listing administrative bodies' obligation to quick and efficient procedure, to explain its actions and, if necessary, to refer the person to the right administrative body, moreover, the openness of general public authorities and their role in balancing conflicting interests as content elements of good administration (Overview of the activities of the Chancellor of Justice in 2005 p 252). However, only a year later, the Chancellor of Justice has noted that "*the principle of good administration* contained in section 14 of the Constitution is no longer an incomprehensible concept, but is very clearly reflected in the various procedural acts." (Overview of the activities of the Chancellor of Justice in 2006 p 280).

The various approaches outlined above regarding the value of *good administration* and the content elements of this concept could be continued, however, in the light of the main purpose of the article, the analysis of the sources discussed in the article reveals the most differences between the value and contents of *good administrative practice* / the *practice of good administration* on one hand and between the *right to good administration* and the *principle of good administration* on the other. Such, at times principled and outside the realm of law, concepts of *good administrative practice* / the *practice of good administration* would allow, in Estonian law, the distinction to be made between custom and law, or rather a principle of law. However, taking into consideration the overlap between the content components of practice and law, or of principles of law, one could conclude that the various terms of good administration

are used randomly. The somewhat abstract contents of *good administrative practice* / the *practice of good administration*, shows the most uncertainty about the place of good administration in Estonian law. One could also argue that the case-law-based understanding of *good administrative practice* / the *practice of good administration* does not, at least in part, serve the essential purpose of good administration, which is to specify the general administrative and procedural rights in the field of administrative law (The Constitution of the Republic of Estonia. Annotated edition. Juura 2017, p 203).

Returning to the exemplary case referred to at the beginning of the current section (Judgement of the Administrative Chamber of the Supreme Court of 18.10.2004, 3-3-1-37-04, Clause 8), in which the court assessed the administrative body's actions to be contradicting with, in addition to the *principle of good administration*, also the *practice of good administration*, it is difficult to provide the latter's content through a specific component, thus enabling the *practice of good administration* to be considered synonymous with the *principle of good administration*.

4. A TIME FOR CHANGES IN THE VALUE PROCESS OF GOOD ADMINISTRATION AND ITS CONTENTS IN ESTONIAN LAW

An analysis of the Estonian judicial practice and the practice of the Chancellor of Justice on good administration as a (fundamental) right, principle of law or custom, and the varied content attributed to each of them by case law and the practice of the Chancellor, shows a lack of clear understanding of both, the place and contents of good administration in Estonian law. However, good administration should be the cornerstone of modern administrative procedures. In order for the entire administrative procedure to be able to rely on this cornerstone, it is first necessary to clarify the place of good administration in Estonian law – whether good administration will continue to be specified by judicial practice and the practice of the Chancellor of Justice, and thus remain a legal principle without specific content components or a custom that would enable even broader and more abstract approaches or will good administration become a universally understandable fundamental right, which actually specifies the organisational and procedural rights in the field of administrative law.

The need for clarity about the place and contents of good administration in Estonian law has also been emphasised by U. Lõhmus (Former judge at the European Court of Human Rights and Chief Justice of the Supreme Court of the Republic of Estonia), according to whom, in today's Estonian law, the meaning of good administration is amorphous (U. Lõhmus' Minutes Speech at the meeting of a body of Constitution experts convened by the Minister of Justice via decree No. 110 of 05.12.2016 on 23.05.2018. Ministry of Justice. Tallinn 2018, pp 331-337) and there is no clarity as to what is the core of this right (Ministry of Justice. A body of Constitution experts. Activity report of the body of Constitution experts. IV Fundamental rights and freedoms. Tallinn 2018, p 55). In order to eliminate the existing ambiguity, U. Lõhmus, as a rapporteur of the Constitutional Expert Committee established in 2016 by the Minister of Justice of the Republic of Estonia, has proposed to supplement the Estonian Constitution with a "new right" – *right to good administration*, specifying good administration with an exhaustive list of everyone's

right to have the authorities dealing with his or her question impartially, fairly and within a reasonable time, moreover, with everyone's right to be heard before any individual measure which would affect him or her adversely is taken and with the administrative bodies' obligation to justify their decisions (Ministry of Justice. A body of Constitution experts. Activity report of the body of Constitution experts. IV Fundamental rights and freedoms. Tallinn 2018, p 343). Although the suggested proposal, though not exhaustive, looks similar to the wording of Article 41 of the Charter of Fundamental Rights, it is not a transcription of the content of Article 41 of the Charter into the Estonian Constitution. This article does not focus on the substantive comparison of U. Lõhmus' proposal with Article 41 of the Charter of Fundamental Rights, nor does it analyse the substantive quality of the proposal. However, the Ministry of Justice's subsequent amendment of U. Lõhmus' proposal's wording deserves mentioning – with the aim of submitting them to the Government of Estonia and the Parliament of Estonia for their position (Ministry of Justice. A body of Constitution experts. Activity report of the body of Constitution experts. IV Fundamental rights and freedoms. Tallinn 2018, p 4). This editorial change of Lõhmus' proposal by the Ministry of Justice is minor in form: the proposed amendments state that "everyone has *the right to good administration*. This right includes, in particular: …" (Ministry of Justice. A body of Constitution experts. Activity report of the body of Constitution experts. IV Fundamental rights and freedoms. Tallinn 2018, p 7). However, the addition of only one term, i.e. the term "in particular", to U. Lõhmus' proposal alters the whole concept of good administration's substantial clarity. By leaving good administration's list of contents open, good administration would remain in many respects a right to be specified by judicial practice and would not serve the essential purpose of good administration – to give concrete expression to general organisational and procedural rights in the area of administrative law.

5. CONCLUSION

Unlike in EU law, where the *right to good administration* is referred to and defined in Article 41 of the Charter of Fundamental Rights of the European Union with specific component elements, Estonian law lacks clarity as to the definition and contents of good administration due to the lack of legal regulation in this regard. The ambiguity stems from the broad terminology used in practice: the terms "*the right to good administration*", "*the principle of good administration*", "*good administrative practice*", "*the practice of good administration*" as well as "*the principle of good administrative practice*" are used, without considering that "right", "principle" and "practice" are not synonymous. Although judicial practice and the Chancellor of Justice predominantly value good administration as a fundamental right in Estonian law - irrespective of the applicable term, it would be more appropriate to consider good administration as a legal principle through the *principle of good administration*.

Under different concepts of good administration, Estonian law presents good administration with variations - under different terms there are both overlapping and different content elements. The overlapping elements of "right", "principle" and "practice" are elements with which *the right to good administration* has been exhaustively embodied in Article 41 of the Charter of Fundamental Rights of the European Union and recognised by the Court of Justice as elements of good administration (Judgement of the Court of First Instance of 04.10.2006 T-193/04: Hansa-Martin Tillack vs Commission of the European Communities, Clause 127 and the judgement cited therein). In particular, the elements of good administration overlapping in regard to the contents of "right", "principle" and "practice" enable the possibility to infer the random use of different good administration related terms to Estonian judicial practice. The long-standing ambiguity in the value and contents of good administration confirms the necessity for legal clarity. In order to value *the right to good administration* as a fundamental right understandable for everyone, the founding document of the Estonian state - the Constitution - needs modernisation. However, in order for such a fundamental right to have intrinsic value in terms of ensuring the protection of subjective rights, good administration needs clear and framed content – either by

following the lead of the near 20-year old Charter of Fundamental Rights or by filling it with a clear list of contents based on case law and the practice of the Chancellor of Justice. Only in this way can good administration fulfil its essential purpose – to specify general organisational and procedural rights in the field of administrative law.

Contact:

Sille Allikmets
E-mail: sille.allikmets@aaviklaw.ee

REFERENCES AND SOURCES

J. Laffranque. Co-existence of the Estonian Constitution and European Law. Juridica III/2003.

U. Lõhmus. Fundamental Rights and General Principles of EU Law: Functions, Scope and Range. Juridica IX/2011.

The Constitution of the Republic of Estonia. Annotated edition. Juura 2017.

EU Charter of Fundamental Rights. OJ 2012/C 326/02.

Explanations on the Charter of Fundamental Rights. „Explanations on Article 51 - Scope". – ELT C 303, 14.12.2007.

Resolution 77 (31) of the Council of Europe, „On the Protection of the Individuals in Relation to the Acts of the Administrative Authorities.

The Constitution of the Republic of Estonia. RT 1992, 26, 349.

Chancellor of Justice Act. RT I 1999, 29, 406. English text available at https://www.riigiteataja.ee/en/eli/527112018002/consolide (14.10.2019).

Ministry of Justice. A body of Constitution experts. Activity report of the body of Constitution experts. IV Fundamental rights and freedoms. Tallinn 2018. [Online source] Available from: https://www.just.ee/et/uudised/pohiseaduse-asjatundjate-kogu-tegevusaruanne-pakub-vastuseid-eesti-riikluse-kindlustamiseks. [Accessed on 26.08.2019].

Overview of the activities of the Chancellor of Justice in 2003-2004. [Online source] Available from: https://www.oiguskantsler.ee/sites/default/files/6iguskantsleri_2003._aasta_tegevuse_ylevaade.pdf [Accessed on 16.10.2019].

Overview of the activities of the Chancellor of Justice in 2004. Tallinn 2005. [Online source]

Available from: https://www.oiguskantsler.ee/sites/default/files/6iguskantsleri_2004._aasta_tegevuse_ylevaade.pdf [Accessed on 17.10.2019].

Overview of the activities of the Chancellor of Justice in 2005. Tallinn 2006. [Online source] Available from: https://www.oiguskantsler.ee/sites/default/files/6iguskantsleri_2005._aasta_tegevuse_ylevaade.pdf [Accessed on 17.10.2019].

Overview of the activities of the Chancellor of Justice in 2006. Tallinn 2007. [Online source] Available from: https://www.oiguskantsler.ee/sites/default/files/6iguskantsleri_2006._aasta_tegevuse_ylevaade.pdf [Accessed on 16.10.2019].

Overview of the activities of the Chancellor of Justice in 2008. Tallinn 2009. [Online source] Available from: https://www.oiguskantsler.ee/sites/default/files/6iguskantsleri_2008._aasta_tegevuse_ylevaade.pdf [Accessed on 16.10.2019].

Overview of the activities of the Chancellor of Justice in 2009. Tallinn 2010. [Online source] Available from: https://www.oiguskantsler.ee/sites/default/files/Ylevaade%202009.pdf [Accessed on 16.10.2019].

Overview of the activities of the Chancellor of Justice in 2010. Tallinn 2011. [Online source] Available from: https://www.oiguskantsler.ee/sites/default/files/6iguskantsleri_2010._aasta_tegevuse_ylevaade.pdf [Accessed on 16.10.2019].

Overview of the activities of the Chancellor of Justice in 2012. Tallinn 2013. [Online source] Available from: https://www.oiguskantsler.ee/sites/default/files/ylevaade_2012_0.pdf [Accessed on 17.10.2019].

Overview of the activities of the Chancellor of Justice in 2014. Tallinn 2015 [Online source] Available from: https://www.oiguskantsler.ee/sites/default/files/ylevaade_2014.pdf [Accessed on 17.10.2019].

Judgement of the Court of First Instance of 04.10.2006 T-193/04: Hansa-Martin Tillack vs Commission of the European Communities.

Opinion of Advocate General Wathelet in court case Marchiani vs parliament, ECLI:EU:C:2016:22, C-566/14 P.

Judgement of the Constitutional Review Chamber of the Supreme Court of 17.02.2003, 3-4-1-1-03.

Judgement of the Administrative Chamber of the Supreme Court of 13.06.2003, 3-3-1-42-03.

Judgement of the Administrative Chamber of the Supreme Court of 25.11.2003, 3-3-1-70-03.

Order of the Administrative Chamber of the Supreme Court of 07.05.2003, 3-3-1-31-03.

Judgement of the Administrative Chamber of the Supreme Court of 18.10.2004, 3-3-1-37-04.

Judgement of the Administrative Chamber of the Supreme Court of 11.12.2006, 3-3-1-61-06.

Judgement of the Administrative Chamber of the Supreme Court of 19.12.2006, 3-3-1-80-06.

Judgement of the Administrative Chamber of the Supreme Court of 11.10.2007, 3-3-1-37-07.

Judgement of the Constitutional Review Chamber of the Supreme Court of 30.09.2009, 3-4-1-9-09.

Judgement of the Constitutional Review Chamber of the Supreme Court of 20.10.2009, 3-4-1-14-09.

Judgement of the Administrative Chamber of the Supreme Court of 18.11.2009, 3-3-1-44-09.

Judgement of the Administrative Chamber of the Supreme Court of 16.12.2010, 3-3-1-83-10.

Order of the Administrative Chamber of the Supreme Court of 22.09.2014, 3-3-1-59-14.

Judgement of the Criminal Chamber of the Supreme Court of 12.10.2016, 3-1-1-65-16.

Tartu Circuit Court judgement of 05.02.2008 in administrative matter No. 3-07-38.

Tallinn Circuit Court judgement of 29.03.2010 in administrative matter No. 3-09-277.

Tartu Circuit Court judgement of 25.05.2012 in administrative matter No. 3-10-2889/46.

Tartu Circuit Court judgement of 20.09.2013 in civil case No. 2-12-10337.

Tartu Circuit Court judgement of 15.10.2013 in administrative matter No. 3-12-1000.

Tallinn Circuit Court judgement of 08.04.2014 in administrative matter No. 3-12-2196.

Tartu Circuit Court judgement of 10.11.2015 No. 3-14-186.

Tallinn Administrative Court judgement of 11.01.2006 in administrative matter No. 3-05-339.

Tartu Administrative Court judgement of 22.12.2006 in administrative matter No. 3-06-2129.

Tartu Administrative Court judgement of 15.03.2007 in administrative matter No. 3-06-2484.

Tartu Administrative Court judgement of 15.03.2007 in administrative matter No. 3-10-769.

Tallinn Administrative Court judgement of 23.05.2007 in administrative matter No. 3-07-315.

Tallinn Administrative Court judgement of 28.12.2007 in administrative matter No. 3-07-912.

Tallinn Administrative Court judgement of 08.02.2008 in administrative matter No. 3-07-1178.

Tallinn Administrative Court judgement of 11.07.2008 in administrative matter No. 3-08-390.

Tartu Administrative Court judgement of 22.09.2009 in administrative matter No. 3-09-220.

Tallinn Administrative Court judgement of 27.01.2011 in administrative matter No. 3-10-1919.

Tartu Administrative Court judgement of 19.10.2011 in administrative matter No. 3-11-870.

Tartu Administrative Court judgement of 15.11.2012 in administrative matter No. 3-12-1000.

Tartu Administrative Court judgement of 02.07.2013 in administrative matter No. 3-13-729.

Tartu Circuit Court judgement of 15.10.2013 in administrative matter No. 3-12-1000.

Tartu Administrative Court judgement of 03.06.2014 in administrative matter No. 3-14-203.

Tartu Administrative Court judgement of 17.11.2014 in administrative matter No. 3-13-2063.

Tallinn Administrative Court judgement of 17.11.2014 in administrative matter No. 3-14-50113.

Tartu Administrative Court judgement of 14.11.2016 in administrative matter No. 3-16-1315.

Tallinn Administrative Court judgement of 15.06.2017 in administrative matter No. 3-16-2636.

Tartu Administrative Court judgement of 18.09.2018 in administrative matter No. 3-17-2076.

INSPECTORS OF THE ENVIRONMENTAL INSPECTORATE CONFUSED WITH THE RIGHT TO APPLY DIRECT COERCION

Ülle Vanaisak, MA
Estonian Academy of Security Sciences
Police and Border Guard College
Lecturer

Keywords: law enforcement related legislation, environmental inspector, police official, direct coercion, special equipment, cut-and-thrust weapon, gas weapon, fire-arm, self-defence.

ABSTRACT

According to the Law Enforcement Act valid in Estonia, the police are the only general law enforcement institution that has a right to use physical force, special equipment or a weapon. The allowed special equipment are handcuffs, shackles, binding means, service animal, technical barrier, means to force a vehicle to stop, water cannon, etc. Police service weapons are firearms, gas, electric shock weapon, pneumatic and cut-and-thrust weapons.

Pursuant to the Environmental Supervision Act, environmental inspectors (hereinafter inspectors) of the Environmental Inspectorate (EI) can apply direct coercion with the means and in the extent stated in specific laws. From amongst the means of direct coercion, a competent official can only use physical force, handcuffs, a service animal and a firearm. Upon performing their duties stated by the legislator, there may be a situation in which the inspector may need to use more means than so far stated in specific acts of law.

In 2014 there was a need to legalise the police official's self-defence regulation. The same should also apply for other public safety officials, incl. EI inspectors, who can risk their life and health while performing their professional duties.

There is an analysis that shows that the number of means of direct coercion the EI inspectors can currently use is not enough to fulfil the tasks stated by the legislator. There is no regulation for the officials' right for self-defence and their direct coercion related training programme needs amending.

INTRODUCTION

According to the valid Law Enforcement Act, physical force, special equipment or a weapon may be used by the police in Estonia. Other law enforcement agencies are allowed to use direct coercion in the cases stated in the law (based on Law Enforcement Act (LEA), 2019, § 75 subsections and 2).

The Environmental Inspectorate is a governmental authority under the Ministry of Environment, whose main task is to conduct state supervision and enforce the powers of the state as and in the extent stated in the law (statutes of the Environmental Inspectorate, 2019, §-s 1 clauses 1, 6, 7 p 1). An EI inspector might need to use direct coercion when conducting state supervision according to 26 specific acts of law (see Table 1), applying measures with dual function (see Code of Criminal Procedure (CCO) §-s 140^1, 140^2 and 217^1, 2019), and performing procedural acts and acts securing criminal proceedings (CCP 217^2, 2019).

The application of direct coercion by different law enforcement institutions has not been studied much. In the commented version of the Law Enforcement Act (Laaring, *et al*., 2017, pp. 219-251) it is focused on the general principles of the application of direct coercion. The studies conducted by Estonian jurists focus on the fundamentals of the application of direct coercion (Laaring 2010, Laaring 2015, Jäätma 2015). Problems related to the application of direct coercion by defence forces have been reflected by S. Kirsimägi (2018) and M. Parts (2018). There is a more detailed approach to the city and rural municipality public order officials' need to apply direct coercion in Ü. Vanaisak's article published in 2018. In the main conclusion of this article, it is stated there is a need to legitimise the respective right, also the conclusion features a list of certain means of direct coercion the law enforcement agency needs in order to fulfil their legal rights (Vanaisak, 2018).

In the explanatory notes to the draft legislation of the LEA, initiated by the Government of the Republic on 16 May 2007, there are a number of agencies stated who besides the police should have a right to apply direct coercion, this list also contains the EI. At the same time, it is found that: "If

a law enforcement agency is lawfully given a right to apply certain special measures and the measure foresees the application of direct coercion, the agency then has a right to apply direct coercion in the framework of the respective measure." (LEA explanatory notes to draft legislation 49, 2007, pp. 105). The problem is that the laws assigning the EI inspectors a right to apply direct coercion are contradictory and therefore cause unnecessary uncertainty upon performing official duties – according to the principle of legal clarity, a regulation should give its implementer clear directions. For example, in the so called stem act, Environmental Supervision Act, it is stated that an inspector whose duty is to protect standing crop, game and fishery resources, is allowed to carry a service weapon and use a service dog and handcuffs when performing their official duties (EnvSA, 2019, § 15 subsection 1). At the same time, according to the Hunting Act, they have a right to use physical force, but cannot use a service dog (HA, 2019, § 47[3]). According to the Nature Conservation Act and Waste Act, they can only use physical force. According to Product Conformity Act and Liquid Fuel Act, the application of direct coercion has no regulations whatsoever (see Table 1).

On 17 March 2014, the Chancellor of Justice at that time proposed to ministers to legalise the police official's self-defence regulation, and to analyse what was related to the State Liability Act. The same should also apply for other law enforcement officials who might risk their life and health while performing their duties (Teder 2014, pp. 1). Currently there are no regulations for EI inspectors' rights to use self-defence while performing their duties.

TABLE 1. Acts of law that assign EI inspectors the compentency of conducting state supervision and allow them to apply measures, use the means of direct coercion and give them the competency of proceeding with misdemeanour matters (compiled by Vanaisak).

	ACT OF LAW	APPLICABLE MEASURES														MEANS OF DIRECT COERCION						
		§ 28	§ 30	§ 31	§ 32	§ 44	§ 45	§ 46	§ 47	§ 49	§ 50	§ 51	§ 52	§ 53		PHYSICAL FORCE	SERVICE DOG	HANDCUFFS	SERVICE WEAPON	COMPENTENCY OF PROCEEDING MISDEMEANOUR MATTERS
		PRECEPT	QUESTIONING AND REQUIRING OF DOCUMENTS	SUMMONS AND COMPELLED ATTENDANCE	ESTABLISHMENT OF IDENTITY	PROHIBITION ON STAY	STOPPING OF VEHICLE	DETENTION OF PERSON	SECURITY CHECK	EXAMINATION OF MOVABLE	ENTRY INTO PREMISES	EXAMINATION OF PREMISES	TAKING INTO STORAGE OF MOVABLE	SELLLING OR DESTRUCTION OF MOVABLE TAKEN INTO STORAGE	CONTROL TRANSACTION					
1.	Environmental Supervision Act (ESA)																X	X	X	X		
2.	Atmospheric Air Protection Act (AAPA)		X	X	X					X	X	X	X	X		X				X		
3.	Biocidal Products Act (BPA)		X	X	X		X			X	X	X								X		
4.	Building Code (BC)		X	X	X					X	X	X	X							X		
5.	European Union Common Agricultural Policy Implementation Act (EUCAPIA)		X	X	X					X	X	X	X	X								
6.	Contained Use of Genetically Modified Micro-organisms Act (CUGMMOA)		X	X	X					X	X	X				X						

7.	Release into Environment of Genetically Modified Organisms Act (REGMO)		x	x	x		x	x		x	x	x	x	x				x
8.	Hunting Act (HA)		x	x	x		x	x	x	x	x	x	x	x		x	x	x
9.	Waste Act (WA)		x	x	x		x	x		x	x	x	x	x				x
10.	Fisheries Market Organisation Act (FMOA)		x		x					x	x	x	x					x
11.	Fishing Act (FishA)		x	x	x		x	x	x	x	x	x	x	x		x	x	x
12.	Chemicals Act (ChemA)		x	x	x	x	x			x	x	x	x	x				x
13.	General Part of the Environmental Code Act (GPEnvCA)		x	x	x			x			x	x		x				x
14.	Environmental Monitoring Act (EnvMA)		x	x	x					x	x	x			x 32, 49, 50			x
15.	Radiation Act (RA)		x	x	x		x			x	x	x	x	x				x
16.	Nature Conservation Act (NatCA)		x	x	x		x	x		x	x	x	x	x				x
17.	Animal Protection Act (APA)		x	x	x		x			x	x	x	x	x				x

18.	Earth's Crust Act (ECA)		x	x	x		x			x	x	x			x			x
19.	Forest Act (ForA)		x	x	x		x	x		x	x	x	x		x	x	x	x
20.	Packaging Act (PackA)		x	x	x					x	x	x	x					x
21.	Ports Act (PortA)		x	x	x					x	x	x			x			x
22.	Product Conformity Act (PCA)		x	x	x					x	x	x		x				x
23.	Fire Safety Act (FSA)		x	x	x		x	x			x		x					
24.	Industrial Emissions Act (IEA)		x	x	x			x		x	x	x			x			x
25.	Liquid Fuel Act (LFA)		x	x	x	x				x	x	x						x
26.	Water Act (WaterA)		x	x	x		x			x	x	x			x			x
27.	Public Water Supply and Sewerage Act (PWSSA)		x	x	x					x	x	x			x			x

1. RESEARCH METHODS AND CONDUCTING OF THE RESEARCH

1.1. THE PURPOSE AND THE METHOD

The aim of the study is to analyse the sufficiency of the means of direct coercion in the acts of law regulating the duties of EI inspectors, but also their right to apply the means of direct coercion in the event of self-defence.

First the meaning and aim of the regulations focusing on direct coercion and self-defence are found out, the techniques for the interpretation of law are used, and respective scientific literature is referred to. Secondly, experts in the area are interviewed in order to obtain additional information on the needs of applying direct coercion, on the sufficiency of training and about the related cases in their work. Thirdly, an overview of the training of EI inspectors compared to that of police officers is given. Fourthly, for the ones exercising and implementing the rights, behavioural and decision-making rules for situations that foresee the application of direct coercion are developed, incl. the use of a means of direct coercion in self-defence, for which recommendations for amending legal acts and training programmes are developed.

1.2. SAMPLE

The sample of legal provisions consists of the acts of law assigning the EI inspectors the right to apply direct coercion (see Table 1). The paper features acts of law valid on 1 September 2019. The interviewees are the heads of the Environmental Inspectorate bureaus in different counties. They are experts who have work and management experience in the area of environmental protection. The questionnaire consists of 10 questions. Questions 1-4 focus on the background of the respondent – how long he/she has been working as a head of the bureau (state the number of years worked), how many employees does he/she have (state the number), whether he/she has worked in an agency that has a right to exercise

direct coercion (if yes, state the number of years worked there and name of the agency). In question No 5, means of direct coercion are listed, and the respondents are asked to state which means (electric shock weapon, physical force, gas weapon, handcuffs, cut-and-thrust weapon, pneumatic weapon, binding means, means to force a vehicle to stop, service animal, technical barrier, firearm) are seen as necessary to start implementing. The Likert scale is used, whereas the question consists of positive or negative attitudes towards the object, (Fishben & Ajzen, 2015, pp. 87). A 5-point scale ranging from "I see it as very important" to "I don't see it as important at all" was used. Questions 6-10 were open questions and respondents were asked to explain their answers. The questions were the following:

- Should there be separate regulations for applying direct coercion to defend yourself while on duty (if the official's life and health are in danger)?

- Is the direct coercion related training for EI inspectors sufficient at the moment?

- Please describe at least one situation in which you have had to apply direct coercion while on duty.

The documents' review gives an overview of the EI supervisory official's curriculum currently valid at the Centre for Continuing Education of the Estonian Academy of Security Sciences.

1.3. RESEARCH QUESTIONS

In order to meet the objective, the following research questions were formed:

1. Which discords and contradictions are there related to the regulations for the application of direct coercion when comparing what is stated in the Law Enforcement Act and the specific acts of the EI?

2. Which acts of law need to be amended in order to guarantee implementers legal certainty and clarity in situations that call for the application of direct coercion, incl. the use of the means of direct coercion when performing self-defence.

3. Is the current EI supervisory official's curriculum sufficient for acquiring the necessary competence to apply direct coercion?

1.4. RESEARCH TASKS

1. To give an overview of the acts of law according to which the EI inspectors can and could apply direct coercion.

2. To give an overview of the basis and means of the application of direct coercion and to find out the EI inspector's need to obtain a right to use additional means of direct coercion.

3. To interview the EI experts to find out whether there is a need to apply additional means of direct coercion and whether the training has been efficient so far.

4. To find out whether the current EI supervisory officials' training programme contains direct coercion related training in a sufficient amount to guarantee that the inspectors have the respective competency needed for their work.

5. To develop recommendations to amend the respective acts of law and curricula.

2. LAW ENFORCEMENT AGENCIES' RIGHT TO APPLY DIRECT COERCION

2.1. FUNDAMENTALS FOR THE APPLICATION OF DIRECT COERCION

The Law Enforcement Act (hereinafter LEA) states the general rules for applying direct coercion, the specific laws define the peculiarities of different law enforcement agencies and the means of direct coercion allowed for them, however, the basis for applying direct coercion cannot be extended with specific laws since these can only specify and constrain (explanatory notes of the LEA 49, pp 107).

After the Law Enforcement Act was enforced in 2014, there was a clear system of administrative coercive measures – now there was a regulatory framework for applying direct coercion in addition to penalty payment and substitutive enforcement. The application of direct coercion is justified mostly in urgent threat situations where guaranteeing the fulfilling of an obligation to ascertain and counter a threat or to eliminate a disturbance with administrative coercive measures is impossible or not possible at the right time (explanatory notes to LEA 49, pp. 102, LEA § 76 subsection 1). This is an administrative measure which aims to counter disturbances, prevent their harmful consequences and guarantee the taking of an offender in to custody (Koolmeister, Orion 1998, pp. 382). Direct coercion is applied only to enforce the obligation directly connected with a person – a person is forced to do something, no one is acting instead of them. In the case of obligations not related to persons, penalty payment or substitutive enforcement is used (Laaring 2010, pp. 552, 554).

The application of direct coercion has to be:

- Appropriate and in accordance with the aim / suitable for achieving the aim.

- Unavoidable, requires the smallest possible involvement.

- Proportionate towards the aim, not more burdensome than the legal right being protected. The means of administrative coercion can be used multiple times, they can be changed if needed and they are used until the desired aim has been reached. Before applying the coercion (except for in urgent matters) the parties involved need to be issued a precept (delivered an administrative act) to fulfil the obligation, a deadline for fulfilling the obligation must be stated, also the other party must be warned for the coercive measure to be used. Enforcement is allowed when the period for challenging the administrative act has passed or it has been issued for immediate execution and the person has not fulfilled their obligation yet (LEA § 74-78, Laaring, *et al*., 2017, pp. 301).

Direct coercion is applied by the police, other law enforcement agencies are allowed to do so only in the cases stated in specific acts of law (LEA § 75 subsection 1). Initially it was desired to allow only a few law enforcement agencies to apply direct coercion to avoid the possible uncontrollable wilfulness of public authority. Another explanation for that was the lack of special skills, equipment and weapons related training (explanatory notes to LEA 49, pp. 105). However – if a law enforcement agency has a competency to conduct state supervision and an authorisation to apply the measures stated in the LEA, then they also have a right to apply direct coercion to enforce the measures (explanatory notes to LEA 49, pp. 105). The LEA provides 22 special measures for the exercising of which one may apply direct coercion until it is unavoidable to achieve the aim (LEA 2019). There is also an opportunity to apply direct coercion to enforce a general measure – a precept (LEA § 28 subsection 3). Direct coercion cannot be applied to obtain statements, opinions or explanations (LEA § 76 subsection 3), since it is interpreted as torture (Oestmann 2012, pp 52-62).

Means of direct coercion are divided into physical force, special equipment and weapons (LEA § 74). The levels of direct coercion are defined from the most lenient towards harsher dependent on the presumable seriousness of the applicable measure, the regulations have been developed as a system with internal steps, whereas in the case of the most serious means, the bases for applying coercion are significantly narrower (Laaring 2010, pp. 552). There are three procedural steps related to direct coercion (the steps can be avoided only due to the urgent need to counter

an immediate serious threat or eliminate a disturbance (LEA § 76 subsection 2)): first a valid administrative act must be issued to the addressee to obligate them to counter an immediate threat or eliminate a disturbance, then the person is warned and informed of the circumstances of not fulfilling the administrative act and of which means of direct coercion is going to be applied, the third step is the act of applying coercion (Laaring 2010, pp. 552), which means the application of force is first expressed with orders and prohibitions that in the final step are guaranteed with the application of direct coercion (Jäätma 2015, pp. 163).

Physical force is applied in order to physically influence a person, animal or object (LEA, 2019), whereas force is directly carried from the applier of which to the object of direct coercion. For example, holding, pushing, taking a person away, blocking an animal attack, knocking down doors and hand-to-hand fighting techniques. Special means are mainly used to increase or direct the influence of physical force. Special means are directly listed in the act of law, but there are countless things that could be used as special equipment, for example, a service car or tools used to open doors. It is impossible to list all means specifically, however, the type of the means can be determined according to their aim (explanatory notes to LEA 49, pp. 103). According to Weapons Act § 3 subsection 1 clause 1, subsection 2, weapons of officials or service weapons are prescribed by law to government authorities exercising public authority for the performance of their duties (Weapons Act, 2019). Service weapons are divided into firearms, gas, cut-and-thrust, pneumatic and electric shock weapons (Minister of the Interior, 2019, § 2). The means of direct coercion can be applied together, they can be changed if needed, but one always has to make sure the application of force is not excessive (Kuurberg 2016, pp. 528).

2.2. THE ENVIRONMENTAL INSPECTORATE'S PUBLIC ORDER OFFICIAL'S RIGHT TO APPLY THE MEANS OF DIRECT COERCION TO ENFORCE THE MEASURES OF STATE SUPERVISION

The task of the Environmental Inspectorate is to prevent, find out and counter a threat and eliminate disturbances in the area of environmental protection (statutes of the EI § 6, § 7 subsection 1; EnvSA § 2). The EI conducts supervision over the natural environment and natural resources in all areas, should it be the protection of forests, the earth's crust or fish, or problems related to waste disposal, packaging or external air. In the presence of environmental offences, the EI applies the enforcement powers of the state: issues fines, precepts and demands the environmental damage to be reversed (Environmental Inspectorate 2019). The EI has a right to conduct misdemeanour and criminal procedures in the scope of their competency (statutes of the EI, 2019, § 7 subsections 2 and 2^1). In 2018 there were 142 precepts issued according to eight acts of law and 996 misdemeanour procedures registered according to 15 different acts of law (Environmental Inspectorate 2019). Everyday environmental supervision is conducted by the heads of county bureaus (15) and inspectors (Environmental Inspectorate, 2019).

According to the electronic State Gazette, the Environmental Inspectorate has been given a competency to conduct state supervision and apply measures according to 26 different laws. Upon conducting state supervision according to all acts of law, the EI has a right to apply the following measures of processing of personal data: questioning and requiring of documents, summons and the establishment of identity as stated in LEA §-s 30-32. The prohibition on stay as stated in LEA § 44 can only be applied according to ChemA and LFA; the stopping of a vehicle (LEA § 45) according to BPA, REGMO, HA, WA, FishA, GPEnvCA, RA, NatCA, APA, ECA, ForA, FSA and WaterA; detention of a person (LEA § 46) according to REGMO, HA, WA, FishA, GPEnvCA, NatCA, ForA, FSA and IEA; security check (LEA § 47) HA, FishA and FA. It has been allowed to apply the following measures related to movables and premises: examination of movables, taking into storage of a movable and the selling or destruction of the latter (KorS § 49-53). The named measures can be applied according to AAPA, EUCAPIA, CUGMMOA, HA, WA,

FMOA, ChemA, RA, NatCA, APA, ForA and PackA. According to BPA, REGMO, EnvMA, ECA, PortA, FSA, LFA, WaterA and PWSSA the EI can also apply the examination of movables, entry into premises and the examination of premises, but cannot take a movable into storage. According to the PCA a control transaction can be carried out.

Direct coercion can be applied upon applying the measures in the competency of the Environmental Inspectorate, except in the case of questioning, but eight acts of law regulating the work of the EI do not foresee the application of direct coercion at all (BPA, BC, EUCAPIA, FMOA, PackS, PCA, FSA, LFS).

The Environmental Supervision Act (EnvSA) is the stem act of the Environmental Inspectorate and in its § 15 it is stated that an inspector whose duty is to protect standing crop, game and fishery resources, is allowed to carry a service weapon and use a service dog and handcuffs when performing their official duties. Therefore the Hunting Act, Fisheries Market Organisation Act, Fishing Act, Forest Act and Water Act should state the same means of direct coercion, but in the so-called stem law and the named specific laws contain contradictions. In all acts of law (excl. FMOA that lists no rights to apply any means of direct coercion) the application of physical force has been stated as a means of direct coercion, however, physical force has not been stated in the stem law. Logically the HA and FA should reflect the right to use a service dog, the use of handcuffs and a service weapon. The only means of direct coercion allowed according to the WaterA is physical force.

As mentioned above, there are eight laws that do not foresee the application of direct coercion. However, these acts of law (BPA, BC, EUCAPIA, FMOA, PackS, PCA, FSA, LFS) authorise the IE to apply such means of state supervision that may call for the application of direct coercion, e.g. the prohibition of stay (LFS), detention of a person, stopping of a vehicle (FSA). According to almost all of these laws the inspectors have a right to examine a movable, enter premises and examine them, take a movable into storage – all this may also require the application of direct coercion, the use of physical force being the least harsh.

The application of physical force as the only means of direct coercion is allowed according to 14 acts of law and these are AAPA, CUGMMOA,

REGMO, WA, ChemA, GPEnvCA, EnvMa, RA, NatCA, APA, ECA, PortA, FSA, WaterA, PWSSA.

The EI also has the competency of proceeding offences and according to the Code of Criminal Procedure it can also apply such measures with dual functions as the establishment of identity, prohibition on stay and the forcing of a vehicle to stop (CCP §s 140^1, 140^2, 217^1). The right to apply direct coercion to perform procedural acts and secure criminal proceedings has been stated separately (CCP § 217^2) and according to EnvSA § 15 the allowed means of direct coercion are handcuffs, a service dog and a service weapon.

If the legislator has foreseen the application of direct coercion as an opportunity to enforce the measure, then the EI inspectors should have a general right to apply direct coercion, specific laws should therefore provide a definite list of the means of direct coercion. An overview of the acts of law show that there are some according to which the application of direct coercion is not allowed at all or the only measure allowed is physical force (see Table 1). There is a significant contradiction between the Environmental Supervision Act (the so called EI stem law) and specific laws – the EnvSA allows the application of a service dog, handcuffs and a service weapon, the list does not feature physical force that has been allowed in 18 specific laws. Also, the EnvSA does not state the type of service weapon that can either be a firearm, gas, cut-and-thrust, pneumatic or electric shock weapon (in the meaning of Weapons Act § 31 section 1 subsections 1-4, § 11 subsections 1-4, 6). Specific laws can be more specific about the application of direct coercion, this has only been done according to the Environmental Supervision Act that allows the application of the means of direct coercion – physical force – only when there is a need to establish identity, examine movables or enter premises. The inconsistency in the acts of law does not provide legal certainty for the EI inspectors when they need to apply direct coercion.

3. LEGALISATION OF THE RIGHT OF SELF-DEFENCE FOR ENVIRONMENTAL INSPECTORS WORKING TO PROTECT PUBLIC ORDER

3.1. THE RIGHT TO PERFORM SELF-DEFENCE AND THE APPLICATION OF THE MEANS OF DIRECT COERCION WHEN PERFORMING SELF-DEFENCE

During after work hours, a public order official can rely on criminal law related self-defence like a regular person. Self-defence is divided into necessity (an act to avert a direct or immediate danger to the legal rights of the person or of another person) and act of necessity (the damaging of attacker's legal rights with the most lenient means in the defender's hands that has to meet the dangerousness of the attack) (Sootak & Soo, 2014, pp. 145; Penal Code 2019, § 28) and is in conformity with the theory of self-defence according to which the representative of the state powers, just like any other citizen, has a right to defend themselves in terms of self-defence (Sootak 2007,pp. 85; also see Table 2).

Theory	Content and explanation
Public theory	The self-defence defined in criminal law is a general rule and the special rule defined in the specific law shall be applied.
Criminal law related theory	The rights of the representative of state powers to apply legitimate self-defence arise from criminal law and they cannot be narrowed down with specific laws.
Personal protection theory	The representative of state powers, just like any other citizen, has a right to defend themselves in terms of self-defence.
Theory of separation	The criminal law related justifications and the authorisations arising from specific laws fall under different law branches and therefore do not legally depend on each other.

TABLE 2. Self-defence in different theories (Soo & Tarros 2015, pp. 712; Teder 2014, pp. 8-9; Sootak 2007, pp. 85; Kühl 2002, pp. 112-113; compiled by Vanaisak).

On 17 March 2014, Indrek Teder, the Chancellor of Justice, proposed to ministers to legalise the police official's self-defence regulation and to analyse what was related to the State Liability Act. The same should also apply for other law enforcement officials who might risk with their life and health when fulfilling their duties (Teder 2014, pp. 1). Public authorities also have the constitutional right to defend the state and to live (Constitution of the Republic of Estonia § 13, 16; Teder 2014, pp. 4). The analysis also has a connection with the EI inspectors, who may, while carrying out their duties, face a situation in which they are attacked. In a situation where the attack is caused by the official's official activity, not a person. For example, upon detaining a person, the suppression of a person's resistance transforms into the blocking of an attack against an official (Teder 2014, pp. 8, 9). It is important that while fulfilling one's duties, one first has to rely on the regulations for the application of direct coercion as stated in the LEA. In situations which do not allow the application of direct coercion, but in which it is inevitable to protect the official's own life and health, the officials can rely on the penal law related regulation for self-defence (Teder 2014, pp. 16). According to the principle of legal clarity, a legal provision should provide officials' with clear instructions and certainty they act adequately (Teder 2014, pp. 3; commented version of the Constitution of the Republic of Estonia § 12, subsection 16). For example, assistant police officers have state guarantees if violence is used with regard to them in connection with the performance of their duty and they have been injured, what is more, it has been clearly stated that they can use a firearm or an electric shock weapon for self-defence (Assistant Police Officer Act 2019, § 35, 38). While on duty, a prison service official may use self-defence equipment and physical force to ensure their own safety (Imprisonment Act 2019, § 71 subsection 2). The current Environmental Supervision Act does not have such regulations.

4. HEADS OF THE COUNTY BUREAUS OF THE ENVIRONMENTAL INSPECTORATE ON THE CASES OF APPLYING DIRECT COERCION

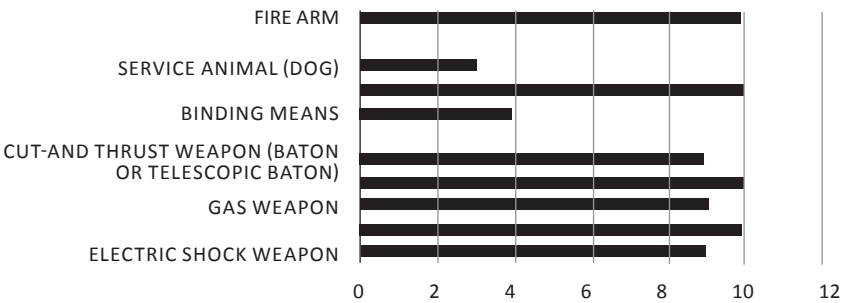
The data collection method used was a survey (questionnaire), which was conducted between 2 and 5 September in the Estonian Academy of Security Sciences Lime Survey environment, where the data of the named study can be found and checked. The questionnaire was sent to 15 heads of the EI county bureaus, 10 fully filled out forms were received (2 were unfinished). On one hand it was convenience sampling since the persons involved were easily accessible (Lagerspetz 2017, pp. 173); on the other hand, they are experts with a task to manage the EI county bureaus. The heads of bureaus who could be reached by telephone were firstly asked for their consent for participation and they were briefly introduced to the content and aim of the survey - the survey was anonymous. All together there were ten questions, the first four of which focused on the experience gained from managing the bureau, the number of employees and their previous experience of working in an organisation that has a right to apply direct coercion. The rest of the questions were connected with the importance of the application of different means of direct coercion, the need to regulate them if they are used in self-defence and the sufficiency of the training. Open questions allow the recipients to explain their answers and provide examples.

The background of the heads of the bureaus was the following: the greatest number of years of being a head of an EI bureau was 20 and the smallest was one. Three of the heads who were less experienced in being a head of a bureau had previously worked 12-23 years in the police or border guard field, therefore in an organisation that has a right to apply direct coercion. The average number of years working as a head of a bureau was 7.6 years. There are approximately seven people working under the heads, the smallest number of employees was four and the largest 11.

The respondents were presented with a list of the means of direct coercion and asked to indicate the importance of them. The levels were indicated on the Likert scale (Armstrong 2006) that ranged from "very important" to "not necessary at all". At the moment the inspectors can

apply such means of direct coercion as physical force, handcuffs, service animal (dog) and a firearm. Current acts of law do not allow inspectors the use of binding means, technical barriers, means to force a vehicle to stop, gas weapons, pneumatic weapons, cut-and-thrust weapons (e.g. baton or telescopic baton) and electric shock weapon; however, according to the characteristics of the measures, it could be necessary to use them while on duty.

According to the survey, there seems to be the greatest need to use physical force, handcuffs and a firearm. Currently the application of these means is allowed according to some acts of law (see Drawing 1). Surprisingly the using of a service dog is not seen as very necessary, the answers might reflect the fact that at the moment the EI does not have any dogs. None of the acts of law allow the application of the means of forcing a vehicle to stop, but according to the respondents, the need for that is the greatest. This is followed by the need to use an electric shock weapon, binding means and a cut-and thrust weapon. Having a right to apply a technical barrier or a pneumatic weapon is not seen as important. The need to make the choice of the applicable means of direct coercion more versatile is mainly seen by the heads of bureaus with a longer working experience (10 years or more) and those respondents who have been heads for a shorter period, but have previously worked at the PBGB for 15-23 years.



DRAWING 1. The importance of direct coercion according to the heads of different bureaus, the lower scale indicates the importance of the application of the means. 10 refers to "extremely important" and 0 to "not important at all" (compiled by the author).

Eight officials of the ten found that the application of direct coercion to perform self-defence while on duty (when the official's life and health can be in threat) has to be regulated more. Two respondents did not see the additional regulation as necessary (See Table 3).

TABLE 3. Respondents answers and examples for the question "Should there be separate regulations for applying direct coercion to defend yourself while on duty (if the official's life and health are in danger)?" (compiled by Vanaisak, 2019).

Unnecessary	Necessary	
"If an official has a right to wear a weapon, they therefore have a right to use it and of course they can perform self-defence. Why wear a piece of equipment if you cannot do anything with it."	"There has to be a regulation, but it cannot be too complicated nor clumsy and finally lead to a situation in which an inspector does not understand where and when they can apply direct coercion ."	"Since the application of direct coercion is always connected with the limiting of the other person's freedoms, it is necessary to have a proper regulation so the official would know exactly in what extent they could apply it. In addition to that, it provides certainty for the person that no one is exceeding the limits of direct coercion."
"Self-defence is regulated and it is allowed for everybody."	"I think that since there are many inspectors, they all have different life experience, education and mental preparation, it would be good if there was a regulation for the application of direct coercion in order to have a more uniform understanding and code of conduct".	"I think that even if an official's life and health are in threat, they must precisely know the extent to which they can apply direct coercion and as many such situations should be played through at trainings."
"Self-defence is also already regulated in the Penal Code, and while on duty self-defence cannot be regulated in any other way."	"If an official's life is in threat and there is an opportunity to use a weapon, it has to be regulated with a law."	"A more detailed description would be necessary so the officials would think the topic through for themselves beforehand."
"In my opinion, when being on duty it is not self-defence, but blocking of an attack, and then there are already other acts of law that regulate that."	"Since our opponents usually have many arguments to demonstrate how they were wrongly treated, it is good if there was at least some kind of regulation for the officials' behaviour."	"In order to avoid situations in which the application of direct coercion is unreasonable, at the same time the regulation cannot be too limiting and ambiguous."

Nine respondents found the training to apply direct coercion insufficient, only one saw it as sufficient. Mostly the need to apply direct coercion is seen in the areas of fishing, hunting and forestry where the damages are great, and the offenders do not obey and are aggressive towards the inspectors and try to escape. There have also been problems with waste management and fuel sellers. There has been a need to apply direct coercion while entering premises or stopping vehicles. The respondents could provide comments. All respondents emphasized the importance of training. The heads of bureaus indicated that the need to apply direct coercion does not arise often, but the training has to be sufficient should such situations arise (See Table 4).

TABLE 4. Respondents answers and examples to the question "Please describe at least one situation in which you have had to apply direct coercion while on duty." (compiled by Vanaisak, 2019).

"Since last year, different real life situations inspectors might encounter have been played through at trainings. At the same time, there is nothing about behaviour in the case of dangerous attacks and inspectors cannot handle them. There has been a lot of theory, but almost no practice. In addition to that, there are situations in which inspectors have trouble with assertiveness and give up on solving situations since they have no experience. For example, last year there was a situation in which a person refused to allow himself to be identified while he was at a river where salmon live and where illegal fishing takes place, but the inspectors gave up on solving the situation."	"The most typical situations are related to getting away in a car, in which the EI has no capacity to force the vehicle to stop. Currently, we use a reflective circle to stop cars and some bureaus have the so-called "carrot" you can put on a torch, but if a driver does not react to them we cannot do anything. I have experienced myself at least twice when at night-time drivers have ignored the EI's signal to stop and just driven away. Such cases are related to possible cases of illegal fishing or hunting."
"I have chased a fisherman running to escape. There was no dust-up, but I needed to be prepared for that."	"When spotting an inspector, a fisherman starts tampering with documents (proof) and does not react to the order to stop their activity."

"Recently on Peipsi Lake there was a situation in which fishermen who'd had too much alcohol had become aggressive and threw the EI's electronic scale overboard, and physically attacked the inspectors who wanted to stop them. There is another case from the Peipsi area that comes to my mind – inspectors found an illegal fish trap in the lake and placed it on the quay at the port. The owner of the trap wanted to take it away secretly. This situation finished with hand-to-hand fighting and a warning shot was made from the service weapon, which helped to solve the situation."	"During a hunting raid in the fishing season while looking at crayfish in cars I needed to use force."
"As a rule, the most aggressive people we check are fishermen and hunters, but also waste operators. Luckily talking usually helps, put in order to open cars, show things, check the catch and tools we have had to apply direct coercion, physical force, etc."	

The respondents could add something more and provide comments (See Table 5).

TABLE 5. Free answers from respondents on the topic (compiled by Vanaisak, 2019).

"The EI officials need to be explained the difference between direct coercion and self-defence. The younger generation seems to be a little aggressive for my taste. Especially in the situation where training is insufficient."	"If you need to identify a person and they do not cooperate – which means to choose? We call the police."	"In my opinion, the current situation in which the EI has a right to apply physical force, but in most cases handcuffs and a service weapon are not allowed, is not reasonable. It is not logical when an inspector detains a person who e.g. wants to fight or escape, then the inspector has to remain there physically holding the person (e.g. there have been cases where a person carrying waste to the woods has wanted to run away. Basically it is a simple offence, but so much hassle around it)".
"In terms of any kind of coercion and means, it is important that the person against whom it is applied knows it, sees it and believes it. As a rule, you then do not need to apply it. Warning is enough. If the warning, activity and means are realistic, then usually the person does the required activity voluntarily to avoid the inspector applying coercion or means against them."	"The application of direct coercion in environmental supervision has been thought through insufficiently. Since in small bureaus the inspectors need to be relatively universal, they need to know according to which law they act in a certain situation. Therefore, it should be regulated quite uniformly. Inspectors should be trained so they would not exceed the limits of applying direct coercion (would not use a means that is not proportional)."	

The answers and examples provided by the respondents illustrate the need to harmonise the EI's means of direct coercion brought in different acts of law, and to have more specific regulations for the application of direct coercion in self-defence. The current regulations are contradictory and insufficient, there are discords that create confusion, and therefore some situations may remain unsolved.

5. OBTAINING OF THE COMPETENCY TO APPLY DIRECT COERCION ACCORDING TO THE CURRENT CURRICULUM FOR EI OFFICIALS

Upon defining the need for training, it relies on the employee's duties and on the skills they need to perform their duties safely and efficiently (Heller, 2003, pp. 181). The Environmental Inspectorate trains new officials at the Estonian Academy of Security Sciences. There is a special supervisory official's training programme, after the completion of which the trainees acquire the knowledge and skills necessary to carry out the duties of a supervisory official (Estonian Academy of Security Sciences, 2019). The training has been divided into six modules, each 99 academic hours. Karm indicates the need of relating theoretical training with practical, and emphasises that learners can use the matters learned in theoretical subjects when solving practical cases (Karm 2013, pp. 71). Self-defence related training and instructions to use special equipment and a service weapon are largely in a practical format, it lasts 21 academic hours and the assessment criteria have been brought as activities (see Table 3).

According to the current acts of law, the EI inspectors have a right to apply physical force, handcuffs and a service weapon while on duty (see Table 1). Learning outcomes of the curriculum and the learning content support the using of physical force, handcuffs and a firearm, but there is nothing about using a service dog as a special equipment. When compared to the curriculum of police officers, the volume of the basic training for EI officials is little. The volume of the police officer's curriculum's module for the application of direct coercion and security tactics is 9 ECVET, which is 234 academic hours (Estonian Academy of Security Sciences 2019). In addition to that, there is the training for the legal bases for the application of direct coercion and the providing of first aid in the volume of approximately 30 hours. The current volume of the direct coercion related training for EI inspectors only allows for giving an overview of the matter and the lecturer can demonstrate some techniques, which can be practiced, but no skills are created nor consolidated in such a short time. In dangerous situations, where there might be a need to apply direct coercion, the EI inspectors have to make decisions that are

based on reflex movements (Birzer, 2003, pp. 29-42). In order to consolidate reflex skills the so-called repetition method is used. The repetition method is based on repeating one and the same movement, therefore, to acquire a basic skill, the student has to repeat one and the same movement continuously to stay cool and polish the motor program of their muscles (Kiveste 2012, pp. 17).

If the choice of the means of direct coercion applicable by the EI inspectors were made more versatile, and the right to use the means for forcing a vehicle to stop, cut-and thrust weapon, baton or a telescopic baton and a gas or an electric shock weapon were added, then the training volume should definitely be increased.

TABLE 6. Extract from the EI supervisory official's training programme, Module: self-defence, the application of special equipment and a service weapon.

Learning outcome	Learning content	Assessment method	Assessment criteria
- Knows the fundamentals of security tactics and the legal limits of applying physical force. - Implements the techniques of applying physical force and the most basic types of strikes. - Can apply handcuffs and handle a service weapon.	Theoretical part: - Basics of security tactics – distances, hands, positions. - Legal limits of applying force as a supervisory official. Practical exercises: - Falls, coming up, protection on the ground, movements while standing up, strikes with hands and feet, and the protection of them. - Moving away from the attack line. - Detention techniques – alone and in pairs. - Introduction of handcuffs, theory and practice. - The using of handcuffs. Exercises alone and in pairs. - Ways of holding the service weapon, positions, grabbing the holster. - Moving with the service weapon and detention.	The trainee demonstrates to the trainer their skill of performing self-defence and the using of special equipment.	The trainee can explain their choice of applicable self-defence techniques and special equipment and can use them according to the given situation.

6. FINDINGS AND PROPOSALS

The analysis shows that the amount of the means of direct coercion allowed for environmental inspectors is insufficient to fulfil the duties stated by the legislator, also the list of the means of direct coercion in different acts of law is inconsistent and does not have a system, and therefore causes uncertainty upon fulfilling the duties. Answers to the survey indicate that inspectors have had problems with assertiveness and have given up on solving situations since they have not had knowledge of the application of the means of direct coercion. Laaring (2010, pp. 552) brings out that the scale of direct coercion has been developed from the most lenient towards harsher means, but there is no hierarchy in the means authorised for the EI. As a result there are acts of law according to which they can use either physical force or a service weapon, but there is no right to apply the intermediate and more lenient ones such as handcuffs, cut-and thrust or gas weapons. Several laws refer only to the application of physical force and no other means, which could be used if the application of physical force has no effect, have been listed.

Officials' right to perform self-defence upon performing public duties has also not been regulated. According to the survey it is very important.

The curriculum needs to be amended in order to teach the legal bases for the application of direct coercion, and to carry out practical tasks and provide first aid. The respondents brought out that there is a lot of theory, but when playing through incidents, they struggle due to limited training.

The Environmental Supervision Act as the EI stem act should list which means of direct coercion the EI inspectors could apply, both when conducting state supervision procedures and offence procedures, therefore it is important to add all the aforementioned means of direct coercion into the act of law. EnvSA § 15 should thus be amended as follows:

- While performing their duties, a state environmental inspector is allowed to apply the following means of direct coercion: physical

force, handcuffs, a service dog, a means to force a vehicle to stop, a cut-and-thrust, gas and electric shock weapon and a firearm.

- An environmental inspector is allowed to apply the aforementioned means of direct coercion only in extreme events when all other measures have been exhausted.

- An official whose life and health might be in threat while performing their duties may apply the means of direct coercion while performing self-defence, however they must not exceed the limits of self-defence.

According to the principle of legal clarity, a legal regulation must provide an official with clear instructions and assurance to act. While performing their duties, an EI inspector cannot constantly analyse which means of direct coercion, according to which law they can apply to enforce the measure or to secure offence proceedings. According to this principle it is important that the means of direct coercion brought in the EnvSA could also be applied according to all other acts of law (see Table 4). At the same time, some distinctness is necessary. For example, probably it is not reasonable to use a service dog to enforce a measure based on the Building Code, Ports Act, Water Act, Public Water Supply and Sewerage Act. Therefore, an additional marking with a different colour and a question mark have been used in the table (see Table 4).

All respondents brought out the need to amend the direct coercion related specific training and practical training. The suggestions to make the training more efficient are the following:

- It is important to increase the volume of practical training in the current curriculum. Instead of 21 academic hours it should be at least 50 academic hours, then the material is consolidated and motor skills appear.

- A prerequisite for taking the electric shock weapon related training is the passing of a basic training focusing on the application of direct coercion. The volume of the electric shock weapon basic training is 16 academic hours, 6 of which focus on the legal bases for using the electric shock weapon and 10 are meant for practical exercises in simulated situations (similarly to the valid police officers' curricula).

TABLE 7. Proposals to add the means of direct coercion into specific acts of law (compiled by the author).

		MEANS OF DIRECT COERCION								
		PHYSICAL FORCE	SERVICE ANIMAL (DOG)	HANDCUFFS	SERVICE WEAPON (FIREARM)	BINDING MEANS	A MEANS TO FORCE A VEHICLE TO STOP	A CUT-AND-THRUST WEAPON (BATON, TELESCOPIC BATON)	GAS WEAPON	ELECTRIC SHOCK WEAPON
1.	Environmental Supervision Act (ESA)	X	X	X	X		X	X	X	X
2.	Atmospheric Air Protection Act (AAPA)	X	X?	X	X		X	X	X	X
3.	Biocidal Products Act (BPA)	X	X?	X	X		X	X	X	X
4.	Building Code (BC)	X	X?	X	X		X	X	X	X
5.	European Union Common Agricultural Policy Implementation Act (EUCAPIA)	X	X?	X	X		X	X	X	X
6.	Contained Use of Genetically Modified Micro-organisms Act (CUGMMOA)	X	X?	X	X		X	X	X	X
7.	Release into Environment of Genetically Modified Organisms Act (REGMO)	X	X?	X	X		X	X	X	X
8.	Hunting Act (HA)	X	X	X	X		X	X	X	X
9.	Waste Act (WA)	X	X	X	X		X	X	X	X
10.	Fisheries Market Organisation Act (FMOA)	X	X?	X	X		X	X	X	X
11.	Fishing Act (FishA)	X		X	X		X	X	X	X
12.	Chemicals Act (ChemA)	X	X	X	X		X	X	X	X
13.	General Part of the Environmental Code Act (GPEnvCA)	X	X	X	X		X	X	X	X
14.	Environmental Monitoring Act (EnvMA)	X	X	X	X		X	X	X	X
15.	Radiation Act (RA)	X	X	X	X		X	X	X	X
16.	Nature Conservation Act (NatCA)	X	X	X	X		X	X	X	X

17.	Animal Protection Act (APA)	X	X	X	X		X	X	X	X	X	X
18.	Earth's Crust Act (ECA)	X	X	X	X		X	X	X	X	X	X
19.	Forest Act (ForA)	X	X	X	X		X	X	X	X	X	X
20.	Packaging Act (PackA)	X	X?	X	X		X	X	X	X	X	X
21.	Ports Act (PortA)	X		X	X?		X?	X	X	X	X	X?
22.	Product Conformity Act (PCA)	X		X	X		X	X	X	X	X	X
23.	Fire Safety Act (FSA)	X		X	X		X	X	X	X	X	X
24.	Industrial Emissions Act (IEA)	X	X	X	X		X	X	X	X	X	X
25.	Liquid Fuel Act (LFA)	X		X	X		X	X	X	X	X	X
26.	Water Act (WaterA)	X		X	X		X	X	X	X	X	X
27.	Public Water Supply and Sewerage Act (PWSSA)	X		X	X?		X?	X	X	X	X	X?

- If acts of law are added the right to apply additional means of direct coercion, then the training needs to change too. Proposals to amend the curricula arise from the police officer's basic curriculum and are the following (there is no firearm-related training):

TABLE 8: PROPOSALS TO AMEND THE DIRECT COERCION RELATED TRAINING PROGRAMME (COMPILED BY THE AUTHOR).

Learning outcome	Assessment criteria	Volume
- Individually and as a member of a team handles and uses a cut-and-thrust weapon, gas weapon and special equipment, and implements the techniques of self-defence and detention lawfully, safely and efficiently. - Provides emergency medical care.	In the event of an attack, moves away from the attack line, falls safely. Releases themselves from different grasps by using the areas sensitive to pain. Upon blocking a physical attack uses different strikes with the hands and feet; Alone or as a member of a team, safely applies the means of detaining a person that are suitable for the situation and can prevent damaging of one's health and the risk of suffocation upon detaining a person. Upon blocking an attack, uses the special equipment, cut-and-thrust or gas weapon (whichever is suitable for the situation) and provides first aid after using a gas or cut-and-thrust weapon. Individually or as a member of a team applies handcuffs and binding means upon implementing direct coercion, conducts security check. Forces a vehicle to stop with the respective means by following the principles of security tactics. Upon taking a person out from a vehicle and detaining them, follows the principles of security tactics and applies physical force suitable for the situation and places the person into a vehicle.	80 academic hours of practical learning.

EI should deploy continuous trainings in the organisation and systematically test the inspectors' skills to apply the means of direct coercion. Here the PBGB's training programme that includes activities in the event of a sudden attack (TORK), should be taken as an example.

CONCLUSIONS AND RECOMMENDATIONS

It is important to amend the acts of law regulating the work of the EI. The named changes help the environmental inspectors choose the suitable means of direct coercion to protect public order and provide the officials with a legally clear bases to perform self-defence in situations in which their life and health might be in danger while performing their duties. It is also important to enhance training, both when the volumes of basic and continuing training are concerned, and in the terms of regularity and practicality.

There are unreasonably few practitioners involved in the development of the acts of law regulating the work of the EI inspectors. So far there has been a rigid opinion that the EI inspectors should not have any right to apply the means of direct coercion, therefore the choice of the means of direct coercion in different acts of law is chaotic and contradictory (Vaidla 2019). A survey conducted among the heads of the EI county bureaus proves that practitioners can convincingly support the inspectors' need to apply direct coercion. Therefore, it is recommended to conduct a survey among the environmental inspectors of the EI to obtain an overview of the need to amend the list of the applicable measures.

Contact:

Ülle Vanaisak
E-mail: Ylle.Vanaisak@sisekaitse.ee

REFERENCES AND SOURCES

Animal Protection Act (200), RT I, 13.03.2019, 16.

Armstrong, M. 2006. A Handbook of Employee Reward Management and Practice. 2nd edition. London: Kogan Page.

Assistant Police Officer Act (2010), RT I, 13.03.2019, 2.

Atmospheric Air Protection Act (2016), RT I, 13.03.2019, 35.

Biocidal Products Act (2009), RT I, 12.12.2018, 26.

Birzer, M. L. 2003. Theory of Andragogy Applied to Police Training. Journal: *Policing: An International Journal of Police Strategies & Management 26/1,* pp. 29-42. Emerald Publishing.

Building Code (2015), RT I, 19.03.2019, 99.

Chancellor of Justice. 2014. To legalise the police official's self-defence regulation, and to analyse what was related to the State Liability Act. [Online Source] Available at: https://www.oiguskantsler.ee/et/seisukohad/seisukoht/m%C3%A4rgukiri-politseiametnike-h%C3%A4dakaitse%C3%B5igus-ja-vahetu-sunni-rakendamine [Accessed on 08.07.2019].

Chemicals Act (2015), RT I, 12.12.2018, 44.

Contained Use of Genetically Modified Micro-organisms Act (2004), RT I, 15.03.2019, 23.

Earth's Crust Act (2016), RT I, 12.12.2018, 53.

Editorial Board: Madise, Ü., Kalmo, H., Mälksoo, R., Narits, R., Pruks, P., Raidla, J., Vinkel, P. 2017. Commented version of the Constitution of the Republic of Estonia. [Online Source] Available at: https://www.pohiseadus.ee/ [Accessed on 08.07.2019].

Einberg, L. 2009. Koolitusvajaduse analüüsimine organisatsioonis. [Online Source] Available at: http://www.pare.ee/files/Liina_Einberg.doc [Accessed on 05.09.2019].

Environmental Inspectorate, 2019. *Aastaraamat võtab kokku keskkonnajärelevalve tegemised 2018. aastal.* [Online Source] Available at: https://www.kki.ee/et/uudised/aastaraamat-votab-kokku-keskkonnajarelevalve-tegemised-2018-aastal [Accessed on 08.07.2019].

Environmental Inspectorate, 2019. *Järelevalvest üldiselt.* [Online Source] Available at: https://www.kki.ee/et/eesmargid-tegevused/jarelevalvest-uldiselt [Accessed on 08.07.2019].

Environmental Monitoring Act (2016), RT I, 22.12.2018, 11.

Environmental Supervision Act (2001), RT I, 13.03.2019, 81.

Estonian Academy of Security Sciences, 2019. *Police Officer's curriculum.* [Online Source] Available at:https://www.sisekaitse.ee/sites/default/files/inline-files/04.1_Politseiametniku%20%C3%B5ppekava%202018.pdf [Accessed on 08.09.2019].

Estonian Academy of Security Sciences, 2019. *Supervisory official's training programme. Continuing education curriculum.* Tallinn: Estonian Academy of Security Sciences.

European Union Common Agricultural Policy Implementation Act (2014), RT I, 13.03.2019, 50.

Fire Safety Act (2010), RT I, 12.12.2019, 71.

Fishbein, M. & Ajzen, I., 2015. *Predicting and Changing Behavior: The Reasoned Action Approach*. New York and London: Routledge.

Fisheries Market Organisation Act (2014), RT I, 28.12.2018, 37.

Fishing Act (2015), RT I, 06.07.2018, 13.

Forest Act (2006), RT I,13.03.2019, 61.

General Part of the Environmental Code Act (GPEnvCA)

Government of the Republic. 2007. In the explanatory notes to the draft legislation of the Law Enforcement Act. [Online Source] Available at: https://www.riigikogu.ee/tegevus/eelnoud/eelnou/8a9c2286-06fc-65d2-957b-bd9e11a940c4/Korrakaitseseadus [Accessed on 15.09.2019].

Heller, R. 2003. Kõik, mida on tarvis teada ärist ja juhtimisest. Juhi käsiraamat. Tallinn: Kirjastus Varrak.

Hunting Act (2013), RT I, 06.07.2018, 12.

Imprisonment Act (2000), RT I, 13.06.2019, 6.

Industrial Emissions Act (2013), RT I, 15.03.2019, 18.

Jäätma, J. 2015. Ohutõrjeõigus politsei- ja korrakaitseõiguses: kooskõla põhiseadusega. Doctoral dissertation. University of Tartu Press.

Jakobs, G. 2008. On the Border of Legal Orientation: Penal Law for the Enemy. Juridica, IV, pp. 211-218.

Karm, M. 2013. Õppemeetodid kõrgkoolis. Foundation Archimedes. [Online Source] Available at: https://www.digar.ee/arhiiv/et/raamatud/16243 [Accessed on 05.09.2019].

Kirsimägi, S. 2018. Relvajõudude õigusest kasutada vahetut sundi korrakaitses. Rmt: R. Kroonberg & T. Roosve & S. Kirsimägi, edit-s. *Sisekaitseakadeemia teadusartiklid nr 2*, pp. 59-73. Tallinn: Estonian Academy of Security Sciences.

Kiveste, R. 2012. Politsei väljaõppe metoodika äkkrünnakute lahendamiseks. Master's thesis. Estonian Academy of Security Sciences.

Kühl, K. 2002. *Karistusõigus. Üldosa.* Tallinn: Juura.

Kuurberg, M. 2016. Estonia Marks 20 years as Party to the Convention on Human Rights. Juridica, VII, pp. 520 – 532.

Laaring, M. 2010. Direct Coercion as an Administrative Coercive Measure in the Police and Border Guard Act and the Public Order Defence Act Bill. Juridica, VIII, pp. 549 – 556.

Laaring, M. 2015. Eesti korrakaitseõigus ohuennetusõigusena. Doctoral dissertation. University of Tartu Press.

Laaring, M., Pars, S., Kranich, H., Nuka, E. Kiviste, J., Mikiver, M., Roosve, T., Vanaisak, Ü. 2017. *Korrakaitseseadus. Kommenteeritud väljaanne*. Tallinn: Estonian Academy of Security Sciences.

Lagerspetz, M. 2017. Ühiskonna uurimise meetodid. Sissejuhatus ja väljajuhatus. Tallinn: Tallinn University Press.

Liquid Fuel Act (2003), RT I, 15.03.2019, 16.

Minister of the Interior, 2018. *The types of service weapons and their ammunition and munition and the procedure for the handling of and for handing over service weapons, their ammunition and munition and components of firearms.* Regulation RT I, 12.09.2018, 6.

Nature Conservation Act (2004), RT I, 22.02.2019, 21.

Oestmann, P. 2012. Lawful and Unlawful Torture in ius commune Criminal Procedure. Juridica, I, pp. 52-62.

Packaging Act (2004), RT I, 13.03.2019, 103.

Parts, M. 2018. Politsei- ja Piirivalveameti nägemus kaitseväe kaasamisest korrakaitselistesse ülesannetesse vahetu sunni kasutamise õigusega. Master's thesis. Estonian National Defence College.

Police and Border Guard Board, 2017. Training programme TORK (acting in the event of a sudden attack). Available on the PBGB's intranet.

Ports Act (2009), RT I, 15.03.2019, 13.

Product Conformity Act (2010), RT I, 12.12.2018, 67.

Public Water Supply and Sewerage Act (1999), RT I, 22.02.2019, 31.

Radiation Act (2016), RT I, 26.06.2018, 10.

Release into Environment of Genetically Modified Organisms Act (2001) , RT I, 12.07.2014, 44.

Soo, A., Sootak, J. 2014. Right of Self-Defence in the Case-Law of the Criminal Chamber in the Past Decade. Juridica, II, pp. 145.

Soo, A., Tarros, K. 2015. Use of Direct Coercion in Prison in Self-Defence Situations. Analysis under Penal and Administrative Law. Juridica, X, pp. 145.

Sootak, J. 2007. Crisis Resolution in the Estonian Legal System, from a Penal Law Aspect. Juridica, II, pp. 82, 83).

Sootak, J., Pikamäe, P., 2015. *Karistusseadustik. Kommenteeritud väljaanne*. Kirjastus Juura.

Statutes of the Environmental Inspectorate (2008), RT I, 05.07.2019, 5.

Vaidla, V., 2019. *Phone conversation with* Väino Vaidla. *[Interview]* (30.08.2019).

Vanaisak, Ü., 2018. City and rural municipality public order officials as bodies conducting state supervision proceedings – the needs and opportunities for increasing their rights. Journal: Proceedings Estonian Academy of Security Sciences, 17: Versatile Security, pp. 27-71 Tallinn: Estonian Academy of Security Sciences.

Waste Act (2004), RT I, 02.07.2019, 3.

Water Act (1994), RT I, 22.02.2019, 33.

Weapons Act (2001), RT I, 13.03.2019, 142.

CLARIFYING (WICKED) SAFETY PROBLEMS WITH A NETWORK ANALYSIS TOOL

Priit Suve, Ph.D.
Tallinn University
School of Governance, Law and Society
Associate professor of public management

Estonian Academy of Security Sciences
Professor of police theory

Keywords: policing, safety, network analysis, wicked problems

ABSTRACT

In safety issues, the police often deal with a normative side of knowledge. They describe an appropriate way of behaviour. However, many studies analysing safety problems emphasize the importance of contextual behaviour.

This article uses the study of safety in Estonia as an example to test a framework that helps clarify discovered problems and enhance the quality of information needed for decision making in policing, in the context of complexity and uncertainty. The analytical framework used, which was rooted in policy network theory clarified a problem, opened a context, and revealed a lot of hidden data. The revealed games, arenas, and networks from the Estonian study are the specific results of this study, and proof of the value of the used framework in this analysis. Improved quality of the information in using an appropriate tool from outside the field of police is the most important and forward-looking outcome of this study.

INTRODUCTION

The police are struggling with various dimensions of complexity starting from safety issues (see, e.g., Rittel & Webber, 1973) and policing regarding tasks, public demands, strategies, technology, accountability, and resources (see, e.g., Bayley, 2016; Devroe & Terpstra, 2015). Complexity as one fundamental characteristic of the social world (see, e.g., Rittel & Webber, 1974; Coclin, 2006; Head, 2008) is also one of the main challenges of contemporary police education (Rogers & Frevel, 2018). In terms of complexity, Rittel and Webber (1973) defined wicked problems as the most challenging problems facing decision-makers. (Ney & Verweij, 2015, p. 1679) In order to advance possibilities for understanding a particular safety problem in all its complexity, various analytical tools should be tested.

Since the police are expected to be precise and clearly express their vision of safety arrangements, the initial condition and perspective should be clarified. For adequate policing, it is unavoidable to be more precise, look behind cognition-based data, and (at least) structure discovered problems concerning complexity. The reason for that is clarified by Robert Hoppe (2018, p. 20): "Rather an approximate solution to the right problem, than a fully elaborated solution to the wrong problem." Even if some precise problem seems to be similar in different places, the level of complexity (the nature of a problem) can be different (e.g., see the comparison of gun policies on gun violence in the US, Canada, and Australia (Newman & Head, 2017)).

The nature of a problem (simple, complex, or wicked) constrains choices for solutions or possibilities for mitigation of a problem. At the same time, the understanding of structural dimensions of a problem makes further action easier and, more importantly, decreases the chances of failure. If the nature of a problem is clarified, the possibility of failure will decrease. Although safety is often viewed as a wicked problem (Rittel & Webber, 1973; Head, 2008), all the issues of safety may not be wicked. Wicked problems cannot be solved but mitigated, which is a critical difference compared to problems like simple or complex that are solvable.

This article asserts that knowledge from studies offering a general view or list of safety problems can provide more precise information after further analysis. There are possibilities to reveal additional data from these analyses to improve the quality of decision making in policing, and, in this way, decrease the chance of failure.

The primary purpose of this research is to test the concept of the policy network approach (van Bueren, Klijn, & Koppenjan, 2003) as an analytical tool to reveal possible hidden information from the study of "*Estonian's understanding on safety issues*" (Suve, 2016). However, this research is not a critique of the examined study or understandings of safety issues. Also, an attempt to structure safety issues in the social world is a simplification of the latter. For this reason, the concept of the policy network approach is only one possible tool for analysis.

Revealed hidden games, arenas, and networks from the Estonian study, are the specific results of this study, and proof of the value of the used framework in this analysis. The possibility to improve the quality of data available in using an appropriate tool is the most important and forward-looking outcome of this study.

This article consists of five main parts. In the introduction, the research problem, argument, and general overview of the research are presented. The second part clarifies the background of the study in more detail. In the third part, the methods of the study will be presented, and the last two parts are dedicated to discussion and conclusions.

BACKGROUND

THE COMPLEXITY OF SAFETY PROBLEMS.

Why is the question of complexity crucial for policing? There are many reasons for that, but defining the right problem and understanding the nature of the problem (simple, complex, wicked) are crucial factors that decrease the possibility of failure.

Police leaders dealing with contemporary safety issues face at least two different kinds of uncertainties: about the content (what is the actual problem?) and a process (how to deal with the problem?) (see, e.g., Koppenjan & Klijn, 2004). Without a context, it is worthless to try to align these uncertainties according to importance, but structuring a problem clarifies the context. In this article, the structure of a problem is in focus. Trying to solve an unsolvable problem, is not only ineffective, but possibly a stimulus for other problems. Wickedness (see Rittel & Webber, 1973) can be recognised as one of many characteristics of the contemporary world.

In social science, the term "wicked problem" gets increasing attention in many fields like public policy (e.g., Ferlie, Fitzgerald, McGivern, Dopson, & Bennett, 2011; Head & Alford, 2015); management (e.g., Camillus, 2008; Grint, 2010), and network governance (e.g., Van Bueren, Klijn, & Koppenjan, 2003; Weber & Khademian, 2008) to mention only some samples. Safety (with its derivates) is one often-cited example of wicked problems. (See, e.g. Rittel & Webber, 1973; Conklin, 2001; Head, 2008; Camillus, 2008)

Although safety problems are often used as an example of wicked problems, the concept is underestimated and rarely discussed in the literature of policing (see table 1 below). Filling this gap performs many advantages. Clarity of a problem and the context are crucial factors in decision making. For that reason, it is useful to introduce possibilities and approaches from outside the regular field of policing like criminology or police science.

In order to understand the field of overlapping and mixed problems, a problem itself should be spread out as clearly as possible. It could be useful to nail the practice of looking for lenses from other disciplines.

Even if the rhetoric about safety issues may present something else, it is common to take crime statistics as a starting point to value the police. For the police, the crime statistic often appears as a primary source for planning daily work. Since the quantitative data seams simpler to read compared to more abstract and vague understandings of citizens, it may appear as an explanation for this action. However, it does not have to be like this. Presenting citizens' understandings more analytically makes the information more readable and understandable.

POLITICAL SCIENCE MEETS POLICING.

Different views on safety problems, as well as solutions, is a well-known fact. The question is, how these different views can lead to a more comprehensive understanding of a particular problem? This question leads to disciplines like political science and governance, which have long traditions in dealing with complex and wicked issues in society. People are the essential source of knowledge in safety arrangements, and therefore it is vital to know their position and understanding about an issue. It is necessary to use various analytical lenses to "read" data more comprehensively and discover potentially hidden fields and layers that may have valuable knowledge to enhance the quality of policing.

From the point of epistemology, in dealing with wicked problems, the positivist approach is not sufficient. Approaches like interpretivism or constructivism offer extra possibilities in describing and explaining problems in the social world. For these reasons, it is useful to be informed about discussions on wickedness, include the knowledge into conversations about safety in the field of policing, as well as to police vocabulary. The concept of wicked problems in social sciences is known already for more than forty years and has a direct link to policing. Problems of safety are never the same and should be carefully studied before solving them. It is difficult even to imagine a problem of safety that could be solved solely by a single actor (like the police), and - like Loader and

Walker (2007, p. 2) famously stated -, "writing about contemporary security requires one to come to terms with much more than the nation-state and its police, military and cognate security operatives". In police studies, this kind of research design is seldom-used.

For the reasons described above and having an ambitious purpose for more comprehensive knowledge of safety for the sake of the development of policing, it is useful to look at some other fields that have advanced knowledge in these issues. Political science has long traditions in dealing with complex and multidimensional problems that penetrate all of society. Since safety problems are often linked to various disciplines (e.g., education, planning, law, psychology) at various levels (e.g., individual, group, society), the networked nature of the topic is a vital characteristic to keep in mind. The dubious and networked context is also the reason to look towards the more experienced field in dealing with wicked problems from a network perspective. In this article, the analytical framework offered by van Bueren, Klijn, and Koppenjan (Van Bueren et al., 2003) will be presented as one possible tool and will be tested on the Estonian case. In 2016 the Estonian Police and Border Guard Board carried out the study (Suve, 2016) with a purpose to identify how the questions of safety are understood by different domains (education, safety, local municipality, public service, third sector, media) and regions (five of fifteen counties were examined). In this article, the results of this qualitative study will be analysed by using the above stated analytical framework, which is specially designed to analyse complex and uncertain problems. The framework offers the concept to identify policy games (series of interactions between actors), arenas (places where specific groups of actors interact on an issue), and networks (collection of stable relations among mutually dependent actors). (Van Bueren et al., 2003, p. 195)

LITERATURE REVIEW

Extensive use of the idea of wicked problems within various disciplines is presented above, and there is no need to repeat it here. In this section, the appearance of the term "wicked problem" in police literature is under closer examination. The frequency of using the term "wicked problem" does not characterise the actual approaching of wicked problems in a particular field. However, it may characterise the embeddedness of some knowledge from fields related to the term. For example, if the term is rarely used in the field of the police, it does not mean that the police literature is covering only simple or complex (or tame) problems and not dealing with wicked problems. Still, it does indicate the lack of use of the terminology that is familiar to some other field that has a broader audience and better potential, capabilities, or traditions in developing this particular topic. The field of police is narrow and holds less "manpower" (i.e., capabilities) compared to many other fields like political science, management, or even criminology. For these reasons, learning and using knowledge from other disciplines is crucial for the police. Since the police are only one of many players in the field of safety, it is an excellent example to characterise the interdisciplinary ethos enclosing the police. However, this particular ethos refers to the mindset necessary in policing (e.g., focus on cooperation and networks).

The wicked problem as a concept has been developed in a variety of studies starting from the 1970s across several scholarly disciplines (e.g., public management and governance, climate change response policy, health care policy and programs, urban and regional planning, business management (see Head & Alford, 2015, pp. 715-716). Although the problems of general safety, as well as any particular problem of safety, are widely recognised as wicked problems, the topic is rarely used in police literature. For example, a search for the term wicked problem in police journals indexed on Web of Science (WoS) and Scopus, is represented

in Table 1[1]. The results presented, quite explicitly visualise the use of the term in the field of policing.

TABLE 1. The search results for the term wicked problem from Google Scholar and police journals.

Title of journal	Search from Google Scholar published in the journal with all of the words: wicked problem	Search from the homepage of the journal from "anywhere"
Policing & Society	12	13
Police Quarterly	4	4
Policing: An International Journal of Police Strategies & Management	5	4
Police Practice and Research	5	6
Policing: a Journal of Policy and Practice	9	10
Journal of Police and Criminal Psychology	2	2
Journal of Policing, Intelligence and Counter Terrorism	0	1

Source: Google Scholar; the homepages of police journals: Policing and Society. An International Journal of Research and Policy; Police Quarterly; Policing: An International Journal of Police Strategies & Management; Police Practice and Research; Policing: a Journal of Policy and Practice; Journal of Police and Criminal Psychology; Journal of Policing, Intelligence and Counter Terrorism.

Although the concept of a wicked problem - as it is mostly known today - was introduced more than forty years ago (see Rittel & Webber, 1973), its importance in dealing with complex social issues is still rising and continually gets attention in various fields (see Head, 2018). This article contributes to boosting the discussion related to wicked problems in the field of policing.

Rittel and Webber (1973) coined the term "wicked" as a label for the most challenging problems facing decision-makers. (Ney & Verweij, 2015, p. 1679) In the seminal article (Rittel & Webber, 1973), the authors characterised wicked problems as follows:

[1] The reason for using WoS and Scopus as sources for data is simple: these databases cover an influential and extensive number of sources from academic journals. The indexing system is important since the data selected for an academic study should be comparable at least at some level, and WoS and Scopus satisfy these conditions. (See e.g. Meho & Yang, 2007; Aghaei Chadegani et al., 2013)

- There is no definitive formulation of a wicked problem.
- Wicked problems have no stopping rule.
- Solutions to wicked problems are not true-or-false, but good-or-bad.
- There is no immediate and no ultimate test of a solution to a wicked problem.
- Every solution to a wicked problem is a 'one-shot operation'; because there is no opportunity to learn by trial-and-error, every attempt counts significantly.
- Wicked problems do not have an enumerable (or an exhaustively describable) set of potential solutions, nor is there a well-described set of permissible operations that may be incorporated into the plan.
- Every wicked problem is essentially unique.
- Every wicked problem can be considered to be a symptom of another problem.
- The existence of a discrepancy representing a wicked problem can be explained in numerous ways. The choice of explanation determines the nature of the problem's resolution.
- The planner has no right to be wrong.

Since the idea about wicked problems developed in the literature of planning (Peters, 2017, p. 387), it is from that point closely related to the police as one of the most experienced and professional planners and decision-makers on safety issues.

The way how police are organised has a remarkable impact on police behavior (see, e.g., Cordner, 2016). For this reason, the following organisational aspects are emphasized. From an organisational perspective, the term wicked problem has got much attention. The ideas elaborated by Keith Grint (2005) are widely known and complementary to the ideas of this article. Grint conceptualised a hierarchy of problems in

organisational settings and developed a typology of problems, power, and authority. Increasing uncertainty about a solution to a problem (the level of wickedness) is related to the requirement for collaborative resolutions. (Grint, 2005, p. 1477) The latter is useful knowledge in managing every organisation, but certainly has excellent value for the police who are always dealing with various kinds of problems with different complexity. "Successful problem solving requires finding the right solution to the right problem. We fail more often because we solve the wrong problem than because we get the wrong solution to the right problem." (Ackoff, 1974)

METHODS

Networks are a part of our everyday life, but not only. Together with hierarchy and market, the networks can be seen as a particular mental frame of seeing the world. (See, e.g., Meuleman, 2008) Hence, tools designed to analyse networks could be an adequate choice. It does not mean that in a networked society, all problems should be handled through the lenses of the network mindset. However, there are many of these which are worth a try.

Safety is a concept penetrating all (networked) society, and often it is difficult to recognise a particular problem and even associates. These are interrelated concepts, which makes all the situations even more complicated. Thus, defining a problem as well as associates, are both critical concerning the solution. It would be useless to collect or focus on more extensive knowledge without knowing what the problem is. For deciding or choosing what the problem is - since often there are several possibilities to frame the problem -, available information should be elaborated as much as possible. The latter is the challenge of this article.

In dealing with wicked problems, we first should admit the relational nature of social reality. (See e.g., Emirbayer, 1997) Without falling into details regarding relational sociology, it is an overall consensus that social facts are socially constructed. Aaro Toomela (2016, p. 519) stated: "We know that the very same element has a different quality in different structures, and with combining diverse elements into the whole, the qualities of the whole will change." So, the new or changing relations are the causes of change, not entities or facts per se. And from the perspective of safety as a wicked problem, we should keep in mind that "a chaotic social system may appear completely random, but there is always an underlying and generative (real) unplanned order, deeper mechanisms, and hidden figurations (patterns, rules, or norms), which are patiently waiting to be discovered and uncovered […]". (Tsekeris, 2013, p. 102)

Erik Hans Klijn's and Joop Koppenjan's contribution to the research of policy network governance is an acknowledged fact. Together with Ellen van Bueren, they published (2003) an article dealing with wicked

problems in networks and elaborated on the idea that offers one possible solution to the previously stated problem: how to reveal "hidden figurations." Regarding this article, the proposed framework will be tested with the purpose of finding out what are these hidden patterns or structures attendant to particular safety problems (see the case of Estonia below).

There are three central concepts of policy network analysis (van Bueren, Klijn, & Koppenjan, 2003):

1. Games (a series of interactions between actors that focus on influencing problem formulations, solutions, and procedures regarding an approach to a particular policy issue).

2. Arenas (places where specific groups of actors interact on a matter and make choices on specific aspects of the issue).

3. Networks (connection of stable relations among mutually dependent actors).

Networks and arenas are not separated, and policy games can occur in a single arena, but often, it is more complicated. In a policy game, four clusters can be distinguished. (1) Social causes are about the nature of an interaction; is it sufficient for tackling the problem, or new linkages are needed. (2) Cognitive causes are about perceptions and knowledge; what are the possible threats that may result from 'dialogues of the deaf'. (3) Institutional causes are about supportive and facilitative institutions that actors can share (e.g., rules, values, relations, shared languages). (4) Network management concerns strategies or techniques to ensure a working network (e.g., how to reach agreements between parties involved in a policy game). (Van Bueren, Klijn, & Koppenjan, 2003: 195-197)

From that point, the next part will focus mainly on two general tasks:

1. What is known:

- What are the three main games (=safety issues) revealed in the Estonian case?

- What arenas were identified in every 'game'?

- What evidence about possible networks revealed?

2. What is unknown: what is unstated (hidden), but useful knowledge that was revealed in exercising the framework.

Before turning to the discussion of the Estonian case, two particular factors should be highlighted. First, one characteristic of wickedness is person-dependence. It means that even if there is an agreement about a problem, views for solutions may still differ to a great extent. For that reason, the opinion of citizens is essential and should be as precise as possible. Second, problems that initially look similar may have different levels of complexity (see, e.g., the example of gun violence in the US, Canada, and Australia (Newman & Head, 2017)).

DISCUSSION

Testing the network analysis tool on the Estonian case.

The Estonian police from the perspective of the organisation and its tasks is a poorly studied matter. Only lately, have studies been carried out and published in scientific journals. (See e.g., Suve, 2014; Suve, Selg, & Sootla, 2015; Suve, Selg, & Sootla, 2016; Suve, 2017)

An example for this article is the latest analysis (Suve, 2016) and one that tries to engage important players from various domains and regions in the Estonian field of safety to find out their perceptions of safety problems.

Estonia has 15 counties, and five of them were selected for analysis. The counties are divided into municipalities that have significant autonomy to organise the life of its inhabitants. The purpose of the selection, was to encompass knowledge and experiences from perspectives that have a significant impact on social life: size of the district (big (e.g. Harju county) and (small e.g., Saare county); seasonal effects (e.g., Pärnu county as the 'summer capital' and Tartu county as a university town); and cultural factors (e.g, Ida-Viru county as a mainly Russian speaking community, and Saare county as an island separated from possibilities that are natural for citizens on the mainland).

Since there is no existing list of domains that influence safety, and to focus on safety in Estonia at the municipal level, the following domains were selected into the analysis:

- The business sector: four representatives of companies from every county. Two of them from service and two from the production industry.

- The non-profit-making sector: one representative from a youth organisation, one from an elderly organisation and one from a free time organisation from every county.

- The educational sector: from every county one representative from a high-school, one from a vocational school and one from a university (since in Pärnu, Saare, and Ida-Viru county there are no universities, but colleges, the latter was selected for the analysis).

- The criminal justice system: one lawyer, one representative of a prosecutor's office, chief of police, and one judge were selected.

- The public sector: two representatives from public sector organisations in every county were selected.

- The media: from every county one representative from the 'written media' and one from visual media were selected;

- Local government: a county governor and two municipalities (the biggest and a small) from every county were selected.

Document analysis and semi-structured interviews were the methods used in the study. One hundred and one interviews were conducted in total, and qualitative analysis methods were used. Since the interviewees were the leaders of organisations selected for the analysis, the study can be understood as an elite study (in a sense that it grasps people from positions of high responsibility who have a significant influence on social life). The purpose of the latter was to embrace highly influential people from various fields to understand opinions and needs that have a substantial impact on safety arrangements. (Suve, 2016: 6) This sample may also be one of the implications since it grasps people mainly with higher education, and neglects "ordinary" people. However, the latter does not have any impact on this research.

FINDING GAMES, ARENAS, AND NETWORKS.

For a better comprehension of the discussion below, some additional descriptive remarks are vital to emphasize. The question about safety was formulated as follows: What is the most outstanding problem of safety (in 2016)? The following three general safety issues (=games) were identified. The first and most important safety issue for interviewees can

be defined as "an external enemy." The latter had two distinct characteristics: (1) fear about the independence of the state, and (2) vague anxiety regarding immigration and terrorism. The concern related to national security is biased more towards the sphere of security (i.e., has a more state-level character). In Estonian, there are words "turvalisus" and "julgeolek". The former is used most often and in a broader sense, and frequently includes both, safety (e.g., crimes, well-being) and security (e.g., independence of the country). The latter (julgeolek) is mainly used in the context of violent threats to the country (e.g., war). Although the line between safety and security is blurred in many disciplines, in the Estonian term "safety" is mostly used to describe topics related to the police, while "security" is where the military is under discussion.

TABLE 2. The wickedness of the safety issues (games) in Estonia 2016

	Terrorism and the problems related to refugees	**Social problems related to urbanisation, poverty, unemployment, and education**	**Crimes and safety in traffic**
A definitive formulation	No single definition	No single definition	No single definition
An adequate stopping rule	No	No	No
Solution: true-or-false or good-or-bad	Good-or-bad	Good-or-bad	Good-or-bad
Immediate or ultimate test of a solution	No	No	No
Possibility for trial-and-error	No	No	No
An enumerable (or an exhaustively describable) set of potential solutions	No	No	No
The uniqueness	Always unique, and renewing	Constantly renewing	Ever-changing
Possible symptoms of another problem	Segregation, excluded groups	Problems of economic and/or social policy	Distrust, inequality
A discrepancy representing a problem	E.g. local/global	E.g. liberal / conservative perspective	E.g. responsibility of the state or citizens
The implications of a mistake in planning	May be catastrophic for a nation	Huge impact on a state's development	Distrust in society

Source: the author, based on the principles of Rittel & Webber (1973).

Terrorism and the questions related to migration constitute the first group. Problems related to international relations were kept out of the analysis (e.g., Brexit, the war in Ukraine). Social problems related to urbanisation, poverty, unemployment, and education constitute the second group of safety issues affecting the interviewees. The third group consists of criminality and safety in traffic, are these concerns that traditionally belong to the sphere of safety (regarding the police and law enforcement), and were also denoted as an outstanding problem of safety.

Also, the wickedness of the safety issues (games) should be identified since the framework proposed is designed primarily to analyse wicked problems. Without going into detail, the wickedness of the "games" seems to be beyond doubt (see Table 2 below). Because of the limits and the purpose of this article, the detailed assessment of wickedness is not possible or necessary.

The next step for further analysis is to specify the safety issues in order to reveal what was said. The study of safety in Estonia had a specific aim related to safety issues: discover the main problems of safety from the perspective of people whose opinions have a significant impact on social life. It was not designed because of the analytical framework used in this article. For that reason, the study is suitable for this analysis.

The topics of semi-structured interviews were the following: has safety in Estonia changed (since 1991) or how has it changed, and what might be the reasons for that?; What may be the most significant problems related to safety in 3-5 years?; How has the function of the police changed (since 1991)?; And, from the perspective of safety, what expectations do you have of police leaders and/or politicians? It is appropriate to emphasize the general opinion concerning the situation of safety in Estonia in 2016: Estonia is a safe place to live, was the general assumption of interviewees. (Suve, 2016, p. 15)

TABLE 3. The three main problems of safety through the eyes of interviewees

	THE THREE MAIN SAFETY ISSUES (GAMES) IN ESTONIA 2016		
	Terrorism and the problems related to refugees.	**Social problems related to urbanisation, poverty, unemployment, and education.**	**Crimes and safety in traffic.**
Social causes (the nature of interaction)	A branch and organisation based rigid budgeting system together with public-private separation were highlighted as the main sources supporting fragmented governance, and were identified as an obstacle to closer cooperation.		
	The fear related to immigration, was put into highest place only by respondents from the field of municipalities. Representatives from other fields did not see the question as the most important.	Urbanisation leads the way to a widening gap between people due to unequal availability in various domains. An unfortunate integration policy amplifies communication problems between different national groups.	Media and the people - in the case of traffic safety, there is dissatisfaction with the amount of negative information provided by the media.
Cognitive causes (perceptions and knowledge)	People have a need for an expert opinion which would help to orient a huge amount of information and avoid 'dialogues of the deaf'.	Respondents from different age groups and with different educational backgrounds rate the importance of social problems differently by emphasizing different aspects of social problems (e.g. people having a lower secondary education or secondary education did not put the social problems in a high position within safety problems).	People from different educational as well as age groups are often in different positions about the penal policy - the question is about the harsh or soft penal policy.
Institutional causes (supportive and facilitative institutions that actors can share)	A fear and being in the dark concerning the effects of the forthcoming municipal reform in Estonia, but also with the impact of Brexit, were factors that influenced people's opinion about the uncertain institutional environment through the interviews.		

	Traditional actors (from the Estonian point of view) in the field of safety like the police, municipalities, and private security companies were mainly seen as separate and fragmented. The monopoly of the knowledge of safety was often associated with the police, and for this reason, other actors were not seen as trustful.		
	A low level of professionalism in (safety) governance on different levels (e.g. ministries, boards) with low ambitions and ambiguous or unstated purposes causes distrust and complications in knowledge sharing.		
		Diverse language groups (e.g. Russians) with poor knowledge of Estonian reduce (1) possibilities for cooperation and (2) for actual participation in the (market) competition.	
Network management factors (strategies or techniques)	The changing role of the police from a police force to a strategic and equal partner in the field of safety raised a question and emphasized the importance of an ability of local municipalities and other actors in managing and participating in safety networks.		
	The increasing gap between the state and the people, and the lack of using techniques of deliberative democracy were often the pronounced aspects from the perspective of the coherent management of safety issues.		

Source: the author, based on the principles of van Bueren, Klijn, & Koppenjan (2003).

The issues described in Table 3 above indicate that the question of safety is not defined through criminality, but has a broader character, and from that point supports the term used in this article. The results affirm the general understanding that criminality is not the case for most people in Estonia. In autumn 2016, only 3% of Estonian people stated that criminality is the most critical issue for the state. The most important topics were health- and social policy (41%), the economy (33%), and unemployment (24%). From the perspective of this article, it is also important to mention that problems related to immigration also have a significant influence on people (19%). (Ahven et al., 2017, p. 16) For a better understanding of the Estonian context, and particularly from the point of the most crucial safety issue (terrorism and problems related to refugees) it is fruitful to notice that at the time of writing this article, Estonia has not witnessed any terrorist attack in a sense we know from the USA,

London, or Paris. A similar situation may be identified related to the question of refugees - between 1997-2016, Estonia gave a status of refugee to 175 people. (MTÜ Eesti Pagulasabi / Estonian Refugee Council, 2017) Although the total number does not appear to be a problem from the perspective of many other countries (e.g., Italy, Germany, France, or Greece), in Estonia, it is a debatable matter of public opinion. It is complicated to mark the only reason for the latter, but the close history of (occupied) Estonia hides probably some causes for that.

TABLE 4. Identified arenas and networks.

	THE THREE MAIN SAFETY ISSUES (GAMES) IN ESTONIA 2016		
	Terrorism and the problems related to refugees.	Social problems related to urbanisation, poverty, unemployment, and education.	Crimes and safety in traffic.
Identified arenas	Nation states and international alliances (e.g. EU, Interpol)	EU, the Estonian government (incl. the Parliament), county-level municipal governance.	International level (e.g. organised crime and drug problems, political decisions like Merkel's welcome policy); the Estonian government and governmental agencies (e.g. the police) and other organisations (incl. public as well private, but also local government agencies).
Mentioned networks	Networks related to safety (e.g. the police) and economy (e.g. international organisations like the IMF or EU, and decisions of the State on a liberal or conservative scale)	Networks (mainly international) related to the economy, but also state level social policy and economic decisions related to the budgeting of local governments	Networks related to legal systems (e.g. the police, prosecutors office, and courts) and particular environmental aspects (e.g. road services, security companies, drug- and alcohol policy)

Source: the author, based on the principles of van Bueren, Klijn, & Koppenjan (2003).

In order to test and demonstrate the framework, a comprehensive analysis of a particular game, arena, and network is not necessary. However, in order to clarify the context, some remarks about the arenas and networks

described in table 4 above will still be presented. One, and probably the most crucial comment concerns the levels of arenas. The interviewees gave little or no importance to the micro (a person) level in describing safety problems. A similar trend appeared in analysing the network perspective: the attribute-based perspective dominated over an individual-based perspective. The latter means that causes of problems were often seen as rooted in some institutions (e.g., economy) or organisation (e.g., EU) instead of having a relational nature (especially from the individual perspective). (See e.g., Marin & Wellman, 2011)

It can be summarised that the problems, sources of the problems, as well as solutions, are mainly related to "others" than oneself. Discussions often stop at the level of group or organisation or in some other fields or domains.

CONCLUSIONS

Even with all of these challenges, quality policing is crucial. The concept of a policy network approach has been proved in other fields, and now it's great potential in policing has been revealed. It is vital to have a tool with the capacity to get more from the data already gathered. The benefit of this research is not related only to the particular results of the analysis. The research lays out the strength of interdisciplinary thinking and in this way, encourages people from the field of safety to look at and test tools from other disciplines.

However, the results of this research are impressive. The used framework clarified problems as well as opened a context, which could be reported as an instrumental result of this study. The possibility to improve the quality of information dramatically in using an appropriate tool from outside the field of police is the most important and forward-looking outcome of this study. From that point, it may raise a question for police education as well as management. Quality of information for decision making in the context of overall complexity is crucial. The idea and habit of looking for tools outside of a particular field is the necessary precondition for successful policing. Interdisciplinarity is not a buzzword, but has a profound idea behind it. For these reasons, it is useful to be aware of discussions in related fields.

The police are a crucial player in the field of safety and are often expected to say how things should be. The use of the analytical framework presented by van Bueren, Klijn, and Koppenjan (Van Bueren et al., 2003) offers an inspiring example and valuable knowledge for the future.

Although three main safety problems in Estonia were highlighted, terrorism is the one that is the most significant. It is useful to stress that until this study, not a single terrorist act has been carried out in Estonia. Despite that, terrorism was the most critical problem of safety, according to the study. It is an excellent example to illustrate the potential of the proposed framework of analysis. Moreover, terrorism as a concept is often recognised as a wicked problem. (See e.g. Horn & Weber, 2007; Camillus, 2008; Weber & Khademian, 2008; Ranstorp, 2009) In

this article, terrorism was handled as a criminal threat, not as a military act. Although in the literature on terrorism there is not a consensus between the two, the former is more understandable for the police audience. However, terrorism and the case of Estonia are only examples of the introduced framework.

More profound studies from several cases and using different data is needed. In this article, the example is limited to arenas and networks. However, from the perspective of crime prevention, terrorism has its roots in a community - the terrorists are humans, not some abstract entities. The analysis revealed a trend to think that there are 'others' like institutions or policies that have a close and responsible connection to safety. The micro-level (individual) got almost no attention. From the point of safety arrangements and policing, this is probably the most valuable knowledge of this article: it is easy to stick to the inappropriate level of a problem or wrong (visible) problem, which was the apparent threat that arises from the Estonian case. The problem of terrorism was handled only at the international or state level. Both are important in the sense of cooperation, information sharing, or setting the normative and moral context. However, the international and state-level mechanisms can be applied only by and to the people. Concerning networks, a similar gap can be recognised. Terrorism remained handled mainly as problem-related domain like safety and the economy (as attributes!). Both mentioned are essential, but not nearly all that influence terrorism. Domains like social policy (e.g., subsidy, job market), inequality (e.g., tolerance), city planning (e.g., segregation), local policy (e.g., inclusion-exclusion dilemma) also have influence on how local people or immigrants may feel themselves.

Since the article was limited to only one case study and a single type of data, further studies are needed to test and advance the framework of network analysis in the field of policing. It would also be useful to test some combinations of tools for more detailed results for policing, police education, or organisational design.

Contacts:

Priit Suve
E-mail: priitsu@tlu.ee
Phone: +372 502 4585

REFRENCES AND SOURCES

Ackoff, R. L. (1974). Redesigning the future. *New York*, *29*.

Aghaei Chadegani, A., Salehi, H., Yunus, M. M., Farhadi, H., Fooladi, M., Farhadi, M., & Ale Ebrahim, N. (2013). A comparison between two main academic literature collections: Web of Science and Scopus databases. *Journal of Informetrics*, *2*(4), 304–316.

Ahven, A., Kruusmaa, K.-C., Leps, A., Tamm, K., Tammiste, B., Tüllinen, K., Sööt, M.-L. (2017). *Kuritegevus Eestis 2016*. Tallinn: Justiitsministeerium.

Bayley, D. H. (2016). The complexities of 21st century policing. *Policing: A Journal of Policy and Practice*, *10*(3), 163–170.

Camillus, J. C. (2008). Strategy as a wicked problem. *Harvard Business Review*, *86*(5), 98.

Conklin, J. (2001). Wicked problems and social complexity. *CogNexus Institute*.

Conklin, J. (2006). *Wicked problems & social complexity* (p. 11). San Francisco, CA: CogNexus Institute.

Cordner, G. W. (2016). *Police administration*. Routledge.

Das, D. K., & Verma, A. (2003). *Police mission: Challenges and responses*. Scarecrow Press.

Devroe, E., & Terpstra, J. (2015). Plural policing in Western Europe: a comparison. *European Journal on Policing Studies*, *2*, 11.

Donnermeyer, J. F. (2002). Local preparedness for terrorism: A view from law enforcement. *Police Practice and Research*, *3*(4), 347–360.

Dunn, W. N. (1988). Methods of the second type: Coping with the wilderness of conventional policy analysis. *Review of Policy Research*, *7*(4), 720–737.

Emirbayer, M. (1997). Manifesto for a relational sociology. *American Journal of Sociology*, *103*(2), 281–317.

Ferlie, E., Fitzgerald, L., McGivern, G., Dopson, S., & Bennett, C. (2011). Public policy networks and 'wicked problems': a nascent solution? *Public Administration*, *89*(2), 307–324.

Ganor, B. (2002). Defining terrorism: Is one man's terrorist another man's freedom fighter? *Police Practice and Research*, *3*(4), 287–304.

Greene, J. R. (2007). *Encyclopedia of Police Science: 1-volume set*. Routledge.

Grint, K. (2005). Problems, problems, problems: The social construction of 'leadership.' *Human Relations*, *58*(11), 1467–1494.

Grint, K. (2010). Wicked Problems and Clumsy Solutions: The Role of Leadership. In S. Brookes & K. Grint (Eds.), *The New Public Leadership Challenge* (pp. 169–186). Palgrave Macmillan UK.

Head, B. W. (2008). Wicked problems in public policy. *Public Policy*, *3*(2), 101–118.

Head, B. W. (2018). Forty years of wicked problems literature: forging closer links to policy studies. *Policy and Society*, 1–18.

Head, B. W., & Alford, J. (2015). Wicked problems: Implications for public policy and management. *Administration & Society*, *47*(6), 711–739.

Hisschemöller, M., & Hoppe, R. (1995). Coping with intractable controversies: The case for problem structuring in policy design and analysis.

Hoppe, R. (2011). *The governance of problems: Puzzling, powering and participation*. Policy Press.

Hoppe, R. (2018). Rules-of-thumb for problem-structuring policy design. *Policy Design and Practice*, *1*(1), 12–29.

Horn, R. E., & Weber, R. P. (2007). New tools for resolving wicked problems: Mess mapping and resolution mapping processes. *Watertown, MA: Strategy Kinetics LLC*.

Journal of Police and Criminal Psychology. (2017). Springer Link. [Online Source] Available from https://link.springer.com/journal/11896.

Journal of Policing, Intelligence and Counter Terrorism. (2017). Taylor & Francis. [Online Source] Available from http://www.tandfonline.com/loi/rpic20.

Koppenjan, J., & Klijn, E.-H. (2004). *Managing uncertainties in networks: A network approach to problem solving and decision making*. Routledge.

Lagerspetz, M. (2017). *Ühiskonna uurimise meetodid. Sissejuhatus ja väljajuhatus*. Tallinna Ülikooli kirjastus.

Marin, A., & Wellman, B. (2011). Social network analysis: An introduction. *The SAGE Handbook of Social Network Analysis*, *11*.

Meho, L. I., & Yang, K. (2007). Impact of data sources on citation counts and rankings of LIS faculty: Web of Science versus Scopus and Google Scholar. *Journal of the Association for Information Science and Technology*, *58*(13), 2105–2125.

Meuleman, L. (2008). *Public management and the metagovernance of hierarchies, networks and markets: The feasibility of designing and managing governance style combinations*. Springer Science & Business Media.

MTÜ Eesti Pagulasabi /, & Estonian Refugee Council. (2017). Pagulased Eestis. [Online Source] Available from http://www.pagulasabi.ee/pagulased-eestis. (Accessed 08.07.2017).

Newman, J., & Head, B. (2017). The national context of wicked problems: comparing policies on gun violence in the US, Canada, and Australia. *Journal of Comparative Policy Analysis: Research and Practice*, *19*(1), 40–53.

Ney, S., & Verweij, M. (2015). Messy institutions for wicked problems: How to generate clumsy solutions? *Environment and Planning C: Government and Policy*, *33*(6), 1679–1696.

O'Malley, P., & Hutchinson, S. (2007). Converging corporatization? Police management, police unionism, and the transfer of business principles. *Police Practice and Research*, *8*(2), 159–174.

Paterson, C. (2011). Adding value? A review of the international literature on the role of higher education in police training and education. *Police Practice and Research*, *12*(4), 286–297.

Peters, B. G. (2017). What is so wicked about wicked problems? A conceptual analysis and a research program. *Policy and Society*, *36*(3), 385–396.

Police Practice and Research. (2017). Taylor & Francis. [Online Source] Available from http://www.tandfonline.com/loi/gppr20.

Police Quarterly. (2017). SAGE Journals. [Online Source] Available from http://journals.sagepub.com/home/pqx.

Policing: a Journal of Policy and Practice. (2017). Oxford Academic Journals. [Online Source] Available from https://academic.oup.com/policing.

Policing: An International Journal of Police Strategies & Management. (2017). Emerald Insight. [Online Source] Available from http://www.emeraldinsight.com/journal/pijpsm.

Policing and Society. An International Journal of Research and Policy. (2017). Taylor & Francis. [Online Source] Available from http://www.tandfonline.com/toc/gpas20/current.

Powell, C., & Dépelteau, F. (2013). *Conceptualizing relational sociology: Ontological and theoretical issues*. Springer.

Ranstorp, M. (2009). Mapping terrorism studies after 9/11: an academic field of old problems and new prospects. In *Critical terrorism studies* (pp. 27–47). Routledge.

Rittel, H. W., & Webber, M. M. (1973). Dilemmas in a general theory of planning. *Policy Sciences*, *4*(2), 155–169.

Rittel, H. W., & Webber, M. M. (1974). Wicked problems. *Man-made Futures*, *26*(1), 272-280

Rogers, C., & Frevel, B. (Eds.). (2018). *Higher Education and Police: An International View* (1st ed. 2018 edition). S.l.: Springer.

Suve, P. (2014). Kogukonnakeskse politsei roll politsei kujunemisel: arengud Eestis 1991-2013. *Acta Politica Estica*, (5), 42–62.

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

Suve, P. (2017). Do police strategies help promote creative policing? *European Journal of Policing Studies*, *4*, 349–371.

Suve, P., Selg, P., & Sootla, G. (2015). Designing Multidimensional Policing Strategy And Organization: Towards A Synthesis Of Professional And Community Police Models. *Baltic Journal of Law & Politics*, *8*(1), 28–54.

Suve, P., Selg, P., & Sootla, G. (2016). Two Decades of Estonian Police and the (Ir) Relevance of Police Models for the Development of Safety Policy. *Studies of Transition States and Societies*, *8*(1), 36–52.

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

Trifonoff, A., Nicholas, R., Roche, A. M., Steenson, T., & Andrew, R. (2014). What police want from liquor licensing legislation: the Australian perspective. *Police Practice and Research*, *15*(4), 293–306.

Tsekeris, C. (2013). Norbert Elias on relations: Insights and perspectives. In *Conceptualizing Relational Sociology* (pp. 87–104). Springer.

Van Bueren, E. M., Klijn, E.-H., & Koppenjan, J. F. (2003). Dealing with wicked problems in networks: Analyzing an environmental debate from a network perspective. *Journal of Public Administration Research and Theory*, *13*(2), 193–212.

Weber, E. P., & Khademian, A. M. (2008). Wicked problems, knowledge challenges, and collaborative capacity builders in network settings. *Public Administration Review*, *68*(2), 334–349.

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 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

2017

Speech for the Security Research Event 2017. *Julian King, Commissioner for the Security Union*

The echo of terrorism within domains important for the development of the police. *Priit Suve*

TENSOR: Retrieval and analysis of heterogeneous online content for terrorist activity recognition. B*abak Akhgar, Pierre Bertrand, Christina Chalanouli, Tony Day, Helen Gibson, Dimitrios Kavallieros, Emmanuel Kermitsis, Ioannis Kompatsiaris, Eva Kyriakou, George Leventakis, Euthimios Lissaris, Simon Mille, Dimitrios Myttas, Theodora Tsikrika, Stefanos Vrochidis, Una Williamson*

OSINT from a UK perspective: Considerations from the law enforcement and military domains. *Douglas Wells, Helen Gibson*

Elaboration and testing of the methodology of risk assessment and home visit questionnaire for dwellings. *Kadi Luht, Ants Tammepuu, Helmo Käerdi, Tarmo Kull, Alar Valge*

The national critical infrastructure protection program in Poland – assumptions. *Rafał Wróbel, Zuzanna Derenda*

Belief in superstition and locus of control among paid and volunteer rescue workers. *Kristjan Kask*

The role of socializing agents in creating a safer society from the perspective of domestic violence. *Silvia Kaugia*

AUGGMED: Developing multiplayer serious games technology to enhance first responder training. *Jonathan Saunders, Helen Gibson, Roxanne Leitao, Babak Akhgar*

2018

Personality, personal related factors and health related behaviour as predictors of pre-injury risk-taking behaviour in schoolchildren. *Kadi Luht, Margo Klaos, Kenn Konstabel, Diva Eensoo*

City and rural municipality public order officials as bodies conducting state supervision proceedings – the needs and opportunities for increasing their rights. *Ülle Vanaisak*

Understanding Russia's asymmetric approach. *Keith Little*

Combat to smuggling of migrations to EU by sea – sources and potential types of reaction. *Piotr Mickiewicz*

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.

SISEKAITSEAKADEEMIA
ESTONIAN ACADEMY OF SECURITY SCIENCES

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

ISBN 978-9985-67-303-4 (print)
ISBN 978-9985-67-304-1 (pdf)