PROCEEDINGS

Estonian Academy of Security Sciences

■ NUMBER 19 ■ 2020 ■

XIX

OLD AND NEW THREATS – CHALLENGES FOR INTERNAL SECURITY

- Foreword
  Vladimir Sazonov, Kristina Saad
- Internal Security in Poland After 2015. Threats and Responses
  Eugeniusz Cieślak, Zdzisław Śliwa
- Competing Strategic Narratives and Their Reflections in Practice: Russo-Estonian Relations Following the Annexation of the Crimea
  Viljar Veebel, Raul Markus, Liia Vihmand
- Using Military Concepts in Civil Administrative Structures: The Estonian Case
  Diana Marnot
- Understanding the Essence of Ethnic Conflict: A Thematic Literature Review
  Helina Maasing
- The Strategic Interplay between Resilience and Covid-19 Pandemic: Approaches, Assets and Ambitions
  George Mihael Manea
- Improving Policing Through Technology: Comparison of Drone Cameras to Terrestial Scanners in Traffic Accident Data Collection
  Jaanika Puusalu, Andres Mumma
- Developing the Situational Awareness of Incident Commanders: Evaluating a Training Programme Using a Virtual Simulation
  Stella Polikarpus, Tobias Ley, Katrin Poom-Valickis
- The Instrumentalisation of the Mass Media in Russia's Foreign Policy: Cold War versus Contemporary Strategy
  Tomáš Mareš

OLD AND NEW THREATS – CHALLENGES FOR INTERNAL SECURITY

VERBIS AUT RE

PROCEEDINGS

Estonian Academy of Security Sciences

XIX

OLD AND NEW THREATS – CHALLENGES FOR INTERNAL SECURITY

SISEKAITSEAKADEEMIA
ESTONIAN ACADEMY OF SECURITY SCIENCES

Tallinn 2020

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

ISSN 1736-8901 (print)
ISSN 2236-6006 (online)
ISBN 978-9985-67-333-1 (print)
ISBN 978-9985-67-334-8 (pdf)

Printed by:
Auratrükk

www.sisekaitse.ee

CONTENTS

Foreword 5
Vladimir Sazonov, Kristina Saad

Internal Security in Poland After 2015. Threats and Responses 11
Eugeniusz Cieślak, Zdzisław Śliwa

Competing Strategic Narratives and Their Reflections in Practice: Russo-Estonian Relations Following the Annexation of the Crimea 37
Viljar Veebel, Raul Markus, Liia Vihmand

Using Military Concepts in Civil Administrative Structures: The Estonian Case 71
Diana Marnot

Understanding the Essence of Ethnic Conflict: A Thematic Literature Review 93
Helina Maasing

The Strategic Interplay between Resilience and Covid-19 Pandemic: Approaches, Assets and Ambitions 123
George Mihael Manea

Improving Policing Through Technology: Comparison of Drone Cameras to Terrestial Scanners in Traffic Accident Data Collection 163
Jaanika Puusalu, Andres Mumma

Developing the Situational Awareness of Incident Commanders: Evaluating a Training Programme Using a Virtual Simulation 195
Stella Polikarpus, Tobias Ley, Katrin Poom-Valickis

The Instrumentalisation of the Mass Media in Russia's Foreign Policy: Cold War versus Contemporary Strategy 227
Tomáš Mareš

Previous issues 259

Editorial policy and disclaimer 263

FOREWORD

Vladimir Sazonov, Kristina Saad
Editors

It is our pleasure to introduce the nineteenth issue of the *Proceedings of the Estonian Academy of Security Sciences*. The *Proceedings* publish studies of contemporary security issues with an emphasis on internal security and law enforcement. In our current issue, entitled 'Old and New Threats – challenges for internal security', eight articles with authors from Estonia, Poland, Romania, and the Czech Republic focus on different types of security threats and challenges in addition to other relevant topics related to security issues and security environment.

In his classic *The Art of War*, the famous Chinese military thinker, general and strategist Sun Tzu (544–496 BC) emphasised that *'hence to fight and conquer in all your battles is not supreme excellence; supreme excellence consists in breaking the enemy's resistance without fighting"* (Sun Tzu). This well-known expression of an ancient Chinese general illustrates well the nature of modern way of thinking of how to conduct hybrid warfare which has been successfully adopted, for example, by Russia and the modern China in their politics (Renz, 2016).

Over the last decade, the number of different (hybrid) threats and conflicts has significantly increased in the world. However, hybrid threats (often hidden and indirect) are only one part of security threats and

risks which can challenge and damage the modern security environment. Threats which are challenging our world and producing several serious issues might differ in nature, impact factor, significance, influence, and harmfulness. They may only affect a small group of people (e.g. small ethnic or religious groups, subcultures, etc.), but also larger nations and states (Radin, 2017), large regions (e.g. Middle East, Euro-Atlantic region, South-East Asia, etc.), international organisations, ecology, energy, economy, political developments, society, culture, and they might even have a more global effect. One recent example of a crisis with a global impact is the massive spread of the Covid-19 disease which began in China in late 2019 and had conquered most of the world by early 2020.[1] The rapid spread of Covid-19 showed that in addition to numerous imminent military and hybrid threats in different spheres, our modern globalised world also faces a variety of often hidden and unpredictable threats and risks, the impact of which on the global security environment is very difficult to predict (Mölder, Sazonov 2020). Furthermore, some countries (e.g. Russia, China) are using the coronavirus for increasing their influence and achieving their political, economic, or other goals (Rough, 2020; Mölder, Sazonov 2020).

One specific type of threats includes hybrid threats – e.g. information warfare, cyber attacks, political and economic pressure, etc. Hybrid threat is a broad and vague concept; however, it generally stands for the widespread synchronised use of several instruments of power in a range of vulnerable social, economic, political, and public and other functions with the aim of achieving a synergistic effect (Cullen, Reichborn-Kjennerud 2017, p. 3; Sazonov, Koort, Heinsoo, Paas, 2020, p. 11). The well-known term 'hybrid warfare' was largely unknown to the wider public less than ten years ago. Only since the Euromaidan in Kyiv in late 2013 and the annexation of Crimea in February 2014 by the armed forces of the Russian Federation has the wider Western public become aware of 'hybrid' or 'asymmetric warfare'. The term 'hybrid' originates from the Latin word *hybrida,* which stands for *'an individual created from crossing two genetically different individuals, belonging to different types of species or breeds"* (Wetoszka, 2016, 55). Although Colonel William Nemeth of the US armed forces used the term 'hybrid warfare' in his

[1] World Health Organization. Coronavirus 2020, https://www.who.int/health-topics/coronavirus

master thesis already in 2002,[2] it became commonplace in the academic circles much later. Thus, in 2007, Frank G. Hoffman described non-linear warfare as a 'fusion of war forms emerging, one that blurs regular and irregular warfare' (Hoffman, 2007: 7). However, in the current volume, the authors discuss not only hybrid or asymmetric threats because, as we know, there are many other challenges and issues in the security field, such as ethnic conflicts and, last but not least, Covid-19 and its impact on the security environment, etc.

This interdisciplinary volume begins with an overview of the internal security of Poland between 2015 and 2020 by Eugeniusz Cieślak and Zdzisław Śliwa. The authors of this article, titled ***'Internal Security in Poland after 2015. Threats and Responses',*** carry out a preliminary assessment of Poland's response to non-military (hybrid) threats to its internal security and also focus on possible future scenarios related to threats to the internal security of Poland and discuss possible responses to these threats.

The next article, ***'Competing Strategic Narratives and Their Reflections in Practice: Russo-Estonian Relations Following the Annexation of the Crimea'*** by Viljar Veebel, Raul Markus, and Liia Vihmand, analyses the prospects of improvement in terms of economic and political relations between Estonia and Russia against the inert background of reciprocal strategic narratives. The article argues that both Estonia and Russia have a lot to gain from possible improvements in economic relations and from reducing regional security-related tensions.

Diana Marnot's ***'Using Military Concepts in Civil Administrative Structures: The Estonian Case'*** demonstrates the importance of using precise terms from NATO's military concepts by state administrative bodies. To achieve this, historical background for the borrowed terminology is provided and official Estonian, NATO, and EU documents are analysed.

In the article '***Understanding the Essence of Ethnic Conflict: A Thematic Literature Review'***, Helina Maasing provides a roadmap for researchers in the field of ethnic conflict studies. The review is based on a total

[2] Non-linear or hybrid warfare. The term hybrid warfare was used for the first time in his thesis by Nemeth, 2002.

of 96 relevant scientific articles published in English language journals since 1990.

George Mihael Manea's study ***'The Strategic Interplay between Resilience and the Covid-19 Pandemic: Approaches, Assets, and Ambitions'*** explores resilience within international organisations, such as the EU, NATO, and the UN in the context of the present pandemic, with a case study on the Romanian practical experience in trying to reach and increase societal resilience during the first wave of Covid-19.

In the article ***'Improving Policing Through Technology: Comparison of Drone Cameras to Terrestial Scanners in Traffic Accident Data Collection'***, the authors Jaanika Puusalu and Andres Mumma present the results of a field test of drone technology for traffic accident data collection conducted by the Estonian Academy of Security Sciences in September 2019. The results indicate that drone technology bears further study as an alternative to current manual methods.

'Developing the Situational Awareness of Incident Commanders: Evaluating a Training Programme Using a Virtual Simulation' by Stella Polikarpus, Tobias Ley, and Katrin Poom-Valickis presents an analysis of situational awareness training currently implemented as an overall part of the dynamic decision-making model for all rescue incident commanders in Estonia. Based on the adopted Kirkpatrick training programme model, participants were able to accept a new approach to their decision-making training and achieved higher-than-threshold results in all situational awareness levels.

Finally, Tomáš Mareš uses a diachronic perspective in his article ***'The Instrumentalisation of the Mass Media in Russia's Foreign Policy: Cold War versus Contemporary Strategy'*** to carry out a variation-finding comparative analysis to reveal the essential differences between Soviet and current Russian strategies behind the instrumentalisation of foreign mass media on the information-psychological level. The article reveals fundamental differences that stem from varying configurations in the crucial layers of strategy formulation.

In this issue of the *Proceedings of the Estonian Academy of Security Sciences,* the reader will find articles on how old and new threats can

challenge internal security, as well as discussions of using drone technology in traffic accident data collection, using military concepts in civil administrative structures, and a review of literature on ethnic conflicts. The Academy of Security Sciences is continuing to monitor and explore internal security issues from a variety of angles to provide professionals and societies with additional insights into this interesting world.

The journal can be viewed online at https://digiriiul.sisekaitse.ee/handle/123456789/2595 if you would like to see the figures and pictures in colour.

REFERENCES

Hoffman, F. G. 2007. Conflict in the 21st Century: The Rise of Hybrid Wars. Arlington, Virginia: Potomac Institute for Policy Studies, https://www.potomacinstitute.org/images/stories/publications/potomac_hybridwar_0108.pdf [accessed: 23 October 2020].

Mölder, H. Sazonov, V. 2020. The Kremlin's strategic narratives towards the Baltic states during the Covid-19 crisis. – Belonna Quarterly (forthcoming)

Nemeth, W. J. 2002. Future War and Chechnya: A Case for Hybrid Warfare, Thesis, Naval Postgraduate School, Monterey, California, June 2002, https://core.ac.uk/download/pdf/36699567.pdf [accessed: 20 October 2020].

Radin, A. 2017. Hybrid Warfare in the Baltics: Threats and Potential Responses. Santa Monica: Rand Corporation.

Renz, B. 2016. Russia and 'hybrid warfare'. – Contemporary Politics, Vol. 22, Issue 3, 283-300.

Rough, P. 2020. How China is Exploiting the Coronavirus to Weaken Democracies. – Foreign Policy, March 25. https://foreignpolicy.com/2020/03/25/china-coronavirus-propaganda-weakens-western-democracies/?utm_source=PostUp&utm_medium=email&utm_campaign=20502&utm_term=Editor&fbclid=IwAR20YdPlmmmH8JA8xvH9VvDRaGqKq73-2imqjtg3-jK2QXzMNidQS5Igpb0#39;s%20Picks%20OC&?tpcc=20502 [accessed: 10 October 2020].

Sazonov, V.; Koort, Heinsoo, P.; Paas, K. 2020. Introduction of Hybrid Threats of Internal Security. Tallinn: Sisekaitseakadeemia. https://digiriiul.sisekaitse.ee/bitstream/handle/123456789/2576/2020%2010%20Sisejulgeoleku%20h%C3%BCbriidohtude%20tutvustamine%20ENG%20A4_web.pdf?sequence=1&isAllowed=y [accessed: 29 October 2020].

Sun Tzu. The Art of War. Translated by Lionel Giles, Part III: Attack by Stratagem. http://classics.mit.edu/Tzu/artwar.html [accessed: 12 October 2020].

Wetoszka, A. 2016. An Attempt to Identify Hybrid Conflict, Sõjateadlane. Estonian Journal of Military Studies 2, pp. 54-65.

INTERNAL SECURITY IN POLAND AFTER 2015. THREATS AND RESPONSES

Eugeniusz Cieślak, PhD
Baltic Defence College
Faculty member

Zdzisław Śliwa, PhD
Baltic Defence College
Faculty member

Keywords: Poland, internal security, 2015–2020, threats

ABSTRACT

The objective of the article is to provide a preliminary assessment of Poland's response to non-military threats to its internal security. The article discusses threats to Poland's internal security between 2015 and 2020. The scope of analysis is limited to foreign intelligence operations and espionage, extremisms and terrorism, cyber threats, and economic threats, including corruption. Threat assessment focuses on targets for hostile actions, observed patterns and trends, along with consequences to Poland's internal security. Available data on threats to Poland's internal security is consolidated and analysed. The assessment of response to threats discusses its effectiveness and highlights challenges in responding to new threats. The scope of the article is limited to the Internal Security Agency activities and is based on publicly available official governmental documents along with analytical works published in professional periodicals. Based on observed trends, possible future scenarios related to threats to Poland's internal security are presented, and possible responses discussed.

INTRODUCTION

The destabilisation of the security situation in the Euro-Atlantic area by Russia's actions against Ukraine resulted in an immediate increase in threats to Poland's external and internal security. The unfavourable development of the situation required undertaking and intensifying actions aimed at increasing the possibilities of counteracting security threats in the allied, regional and national dimensions. Hybrid threats have become the key threats to Poland's internal security, the catalogue of which is significantly expanding. In recent years, the blurring of the boundary between intelligence threats and hostile cyber, terrorist and economic activities carried out inside the state has become noticeable. The most serious challenges in the field of Poland's security are related to the aggressive policy of the Russian Federation. In recent years, propaganda and disinformation have been the primary instruments of hybrid activities carried out in the information sphere, especially in cyberspace and on social media (Sazonov and Müür, 2017; Śliwa, 2017). As information warfare tools, they are used to weaken Poland's security and weaken its image and position in international relations. The use and deepening of the existing political divisions as well as the exploitation of extremisms perpetuate divisions among Polish citizens, polarise social moods and weaken resilience to external threats. Extremism has been considered as one of the most dynamically developing threats to Poland's internal security after 2015 that may lead to increased violence and even terrorist attacks in the future. The threat of hostile actions by other states and commercial entities for the economic and energy security of Poland is also growing. This applies in recent years to attempts to take over, block, or discredit key investments for the Polish economy. The scale of threats to the cyberspace of the state, its institutions and citizens, is systematically growing and requires comprehensive response.

The aim of the article is to assess the dynamics of changes in the area of threats to Poland's internal security between 2015 and 2020 and their impact on the security of the state and citizens. The article also discusses the actions taken by the state security services to increase Poland's internal security and outlines a forecast for the development of the situation in the coming years. The analysis is limited to four major threats to internal

security posed by foreign secret services and espionage, extremisms and terrorism, cyber threats and economic threats, including corruption. The article thus only focuses on the Internal Security Agency activities and does not discuss the efforts of the Military Counterintelligence Service nor the Central Anti-Corruption Agency. Threat assessment focuses on gauging their scope and targets, magnitude, patterns and trends along with consequences to Poland's internal security. The analysis is limited to the period between 2015 and 2020 and is based on publicly available information provided by the state security authorities and institutions. Responses to each of the threats is then discussed with the aim of assessing their adequacy and effectiveness. Finally, based on historical developments and emerging trends in the security environment, an initial insight on possible future scenarios related to Poland's internal security in coming years is offered. The article references publicly available government documents, analytical studies by think-tanks, and academic research. The discussion presented here is limited to sources not covered by the confidentiality clause.

1. FOREIGN INTELLIGENCE OPERATIONS AND ESPIONAGE

The geostrategic location of Poland along with its membership in NATO and the European Union attracts the attention of foreign intelligence services, including espionage related to security and other functional areas of the state. This area of security is one of the domains of the Ministry of Internal Affairs (MIA), which is responsible for counterintelligence activities. The Ministry has published an overview of foreign services activities between 2015 and 2019, recognising enhanced threats linking it with so-called hybrid tools to impact security. The disappearing boundary between foreign intelligence information-gathering activities and other activities inside Poland is recognised, and it includes the extended use of cyberspace and especially various social media channels. The situation that Poland has been facing in recent years is not new to the region as evidenced by developments in the Baltic states (Winnerstig, 2014) and Ukraine (Mölder, 2016, pp. 101–106). The main targets of foreign espionage and non-information activities in the past five years have been the energy sector, investments, information sphere, and social networks. Among foreign nations that have conducted intelligence operations in Poland after 2015, two have been recognised as particularly interested in influencing the security situation: Russia (through the means of propaganda and disinformation) and China (Serwis Rzeczypospolitej Polskiej, 2020a). The targets of foreign intelligence operations in Poland range from security and military industry to the economy. The adoption of new technologies and operating procedures by foreign intelligence services has necessitated a more focused and deliberate response. Although the threat of foreign intelligence activities in Poland has been growing steadily since 2015, a large amount of information related to counterintelligence was made public only in 2019. After 2015, three persons have been arrested in Poland in connection with espionage for Russia and two persons on charges of spying for China. In October 2016, the Internal Security Agency detained Mateusz Piskorski, a former member of Polish Parliament and a leader of the pro-Russian political party Change. Piskorski has been facing charges of collaborating with Russian civilian intelligence and Chinese intelligence services. He was found to have received financing for pushing a Russian agenda in Poland (Żaryn,

2019). In 2018, an employee of the Ministry of Energy Marek W. was arrested on charges of spying for Russia and then sentenced to jail and prohibited to work in the public administration for ten years. In 2019, a Chinese citizen Wejing W., who was identified as an agent of a civilian intelligence agency, and a Polish national Piotr D. were detained on charges related to espionage (Serwis Rzeczypospolitej Polskiej, 2020b).

Poland has been facing increasing threats from foreign intelligence influence operations. As the hybrid activities that harm Polish security interests are difficult to identify and classify in legal terms, they usually do not end up in courts. Most frequently, foreign citizens suspected of hybrid activities in Poland face administrative actions while the illegal activities of foreign diplomats are addressed by diplomatic procedures. Since 2015, Poland has expelled five Russian diplomats. Four Russian diplomats were expelled from Poland in 2018 as part of the international reaction to the Skripal poisoning (Serwis Rzeczypospolitej Polskiej, 2020a). In March 2019, information collected by the Internal Security Agency led to the expulsion from Poland of the vice-consul of the Consulate General of the Russian Federation in Poznań. The diplomat was declared a persona non grata and was banned from entering Poland and the Schengen area. The Internal Security Agency found the Russian diplomat to have engaged in activities inconsistent with their diplomatic status which could harm Polish-Russian relations (Żaryn, 2019a). In 2018, a Chinese diplomat was expelled from Poland after the conviction of an agent cooperating with the Chinese intelligence in Sweden. According to the Internal Security Agency, the diplomat in question was the senior officer of a Chinese citizen convicted in Sweden. The Chinese diplomat was banned from entering Poland and the European Union (Żaryn, 2019a).

Over the last five years, Poland has ramped up its efforts in addressing hybrid threats. The Internal Security Agency also effectively counteracts hostile hybrid activity by using administrative procedures, such as entry bans, expulsions, denial of permission to stay, negative opinions on applications for citizenship, or withdrawal of permission to stay. The Internal Security Agency has publicised information related to some of the cases. In October 2017, the Russian scholar Dimitrij Karnuakhov, tied to the Russian Institute of Strategic Studies, a Foreign Intelligence Service affiliated think-tank, was expelled from Poland. Karnuakhov was suspected of conducting hostile information activities against Poland.

In late 2017, the Agency assisted in banning three Russian agents posing as researchers from entering the Schengen area. They turned out to be the masterminds behind pro-Russian projects pushed in Poland (Żaryn, 2019b). A telling example of hybrid threats to Poland's security was a case of an attempt to set fire to the office of the Transcarpatian Hungarian Cultural Association in the small town of Uzhhorod in south-western Ukraine. The perpetrators turned out to be Polish citizens who were used to spoiling Hungarian–Ukrainian relations. The Uzhhorod arson attempt was investigated by the Internal Security Agency, which managed to tie the incident to the Polish pro-Kremlin party Change, whose then-leader has been awaiting trial for espionage and cooperation with Russian intelligence services. The case serves as evidence of the complex relationships between the influence of hybrid threats on internal, national and international security in the region. As the spokesman of the Coordinator of Poland's Security Services observed in 2019, 'Narrowing down Russia's hostile activity to spreading lies in the media is a losing battle' (Żaryn, 2019b). In May 2018, two Russian citizens, Yekaterina C. and Anastasia Z., were detained and deported from Poland while three other citizens of the Russian Federation were banned from entering Poland (Deutsche Welle, 2018). According to the Internal Security Agency, all five had made repeated attempts to engage Polish pro-Russian circles in hybrid activities (Żaryn, 2019a). The extent of administrative procedures used to counter hybrid threats is perhaps better illustrated by statistics. Between 2015 and 2019, a total of 28 foreigners were expelled from Poland for activities against the security and interests of the Republic of Poland (Serwis Rzeczypospolitej Polskiej, 2020a).

Protection of classified information plays an essential role in preventing foreign espionage. The Internal Security Agency is responsible for granting Polish citizens and institutions access to NATO, European Union and European Space Agency's classified information. Between 2015 and 2019, approximately 43 thousand individual security clearances and one thousand industrial security clearances were issued. At the same time, 123 persons were denied access to classified information, and the security clearances of almost one hundred persons were revoked. To support the counterintelligence effort, the Internal Security Agency has been increasing its prevention and educational efforts. The statistics available for the period between 2015 and 2019 show 2.6 thousand counterintelligence courses and as many as 58 thousand course participants (Serwis

Rzeczypospolitej Polskiej, 2020a). This aspect is reinforced by other governmental agencies, especially security services, including armed forces within their areas of responsibility. Such complex approach not only supports the efficiency of counterespionage but also contributes to the resilience of the society and awareness of the wide range of threats resulting from the activities of foreign intelligence services in the territory of Poland and beyond.

Poland will remain subject to foreign intelligence operations in the future. Most likely Russian intelligence services will remain active in both espionage and influence operations. They may also inspire and support malicious hybrid activities against Poland's security interests at home territory and abroad. Experts also highlight the increasing scope and intensity of Chinese intelligence operations in Poland. This evolving threat will require deliberate approach integrating legal, conceptual, and organisational efforts. The Chairman of the Parliamentary Commission for Secret Services has observed that the Polish legal definition of espionage is outdated and not entirely relevant to current security threats (Lesiecki, 2019). The definition needs to be updated to address, among other issues, the role of agents of influence and clarify the relevant parts of the criminal code. Strategic communication is viewed as crucial to Poland's counterintelligence efforts (Raubo, 2020). A number of specialists call for a more robust public communication to increase social awareness of the threats of foreign espionage and influence operations. It may also help to build trust in Polish counterintelligence services and demystify some aspects of their operations (Maciążek, 2019).

2. TERRORISM AND EXTREMISM

Poland has not suffered any large-scale terrorist attack in recent years; however, the country could be targeted by radical, extremist, or even internal radicals. Nevertheless, as Poland does not exist in a vacuum, there 'has been a significant evolution of the terrorist threat in the region, and Poland's membership in the European Union (E.U.) and NATO, as well as the participation of Polish troops in international peace operations, are considered a factor that may increase the risk of terrorist attacks in Poland or against Polish citizens abroad' (U.N. Security Council Counter-Terrorism Committee, 2019). This relates to not only direct attacks but also to Poland's status as the East border of the EU and Schengen area causing interest in using the territory of the country for direct activities and transfer routes in connection with illegal drug trade, human trafficking, arms trade, smuggling, or money laundering. The actual list of possible illegal activities is much longer and all of these could lead to terrorist-type attacks as a revenge to disrupt security system and services. Another factor to consider is the active participation of Poland's armed forces and security services, mainly police, in operations abroad in conflict zones. As their involvement in these areas (such as Afghanistan and Iraq) is directly connected to the activities of terrorist organisations, Poland could be a target for revenge actions. Next, foreign terrorist fighters could try and establish networks inside the country as a staging ground for actions inside Poland or abroad.

Between 2015 and 2019, six people were convicted in Poland for terrorism-related activities. Most of the cases were tied to jihadist terrorism. In 2016, the Internal Security Agency arrested Mourad T., who was involved in organising the Paris bomb attacks in November 2015. Mourad T. was one of the most influential people in the leadership structures of the so-called Islamic State. In 2018, the Moroccan citizen Abdeljalil A.E.K. was sentenced to 8 years in prison. The information gathered by the Polish counterintelligence in relation to his arrest was pivotal to thwarting terrorist attacks in two European countries. In March 2019, Mourad T. was sentenced to 3 years and 8 months in prison (Serwis Rzeczypospolitej Polskiej, 2020b). The Agency also prevented a terrorist attack by Mikołaj B., who was arrested in May 2019 in Warsaw. Mikołaj B. was preparing

to carry out a terrorist attack in a public place as part of his revenge on the opponents to the Islamic religion. In September 2019, a 27-year old Polish citizen was sentenced to four years in prison for participating in a terrorist organisation operating in Syria. In December 2019, the Internal Security Agency detained Maksym S., a radical Islamist who was planning an attack in the town of Puławy. To keep the terrorist threat under control, the Internal Security Agency has been monitoring the situation to prevent uncontrolled returns of foreign fighters to Poland. Those efforts are directed at both Polish citizens and foreigners attempting to travel to other countries via Poland. According to the Agency, there is no indication of the potential terrorist threat from radicals, including Islamic fanatics, decreasing in the near future.

The last five years have seen an evolving threat of right-wing extremist and radical movements using neo-Nazi narratives and posing a direct threat to some ethnic and religious minorities and social groups in Poland. The increasing prevalence of this trend calls for decisive actions against such groups to prevent them from closing ranks with political sympathisers. Rising extremism may cause risks to both the internal security of Poland as well as its reputation abroad. As the right-wing extremists cooperate closely with their counterparts abroad, it makes sense to use administrative measures to limit such cooperation. The Internal Security Agency has publicised information about its activities that aimed at reducing a threat of right-wing extremism. Recently, Anton T., a Swedish citizen and a member of a neo-Nazi organisation who came to Poland for paramilitary training, was expelled from Poland with immediate effect by the decision of the Minister of Internal Affairs and Administration. According to the Internal Security Agency, the man posed a serious, real, and present danger to security and public order in Poland. The man was a member of the neo-Nazi Nordic Resistance Movement, which is seeking to create a National Socialist North European Republic through revolutionary means. Another activist with ties to neo-Nazi circles, a Russian man called Konstantin B., was declared a persona non grata in November 2019 for his continued contacts with the representatives of the Polish extreme right. Konstantin B. planned to use the Polish neo-Nazi circles for illegal activities. In September 2020, Internal Security Agency officers detained a German citizen suspected of participating in an organised crime group operating in Poland and other countries. The detainee, Jurgen K., was active on social media presenting radical anti-system views

and supporting extreme right-wing organisations. During the search of the place of work and residence of the detained man, 1.2 kg of TNT along with ammunition and a tear grenade were found (Infosecurity 24, 2020). The Internal Security Agency has made efficient use of various mechanisms for neutralising terrorist and extremist threats over the past five years. At the request of the Agency, 39 people whose presence in Poland was associated with the threat of terrorism were deemed undesirable in Polish territory and 14 were expelled or obligated to return to their home countries (Serwis Rzeczypospolitej Polskiej, 2020b).

It is worth mentioning that Poland has developed a comprehensive approach for addressing terrorist and extremist threats in recent years. Countering terrorist propaganda has been included as one of the priorities of the Internal Security Agency. As online terrorist propaganda can intimidate societies by publicising brutal acts of violence against innocent people and aims at recruiting more jihadists, there was a need for an adequate response. Two aspects of countering terrorist propaganda have included regulation of the content of internet media and holding responsible those who engage in such propaganda activities. In 2017, based on evidence collected by the Internal Security Agency, Dawid D. was convicted of propaganda activities for a terrorist organisation. In 2018, the Internal Security Agency blocked the official media channels of the so-called Islamic State in the state's internet domains (Serwis Rzeczypospolitej Polskiej, 2020b).

To increase societal resilience to terrorist threats, Poland created the Terrorism Prevention Centre of Excellence in 2018. The Centre has been consolidating efforts of national state security agencies and extending international connections toward common goals of reducing terrorist threats. The Centre has been focusing on counteracting extremist and terrorist threats through ensuring an early response to the first symptoms of radicalisation in the society. The Centre has specialised in terrorism prevention in the broad sense, the key element of which is the dissemination of knowledge of the possibility of preventing adverse security events. For this purpose, the Centre has organised profiled training for officers and employees of secret services, as well as public administrative bodies and other entities. The Terrorism Prevention Centre has sought to become a centre of excellence that brings together the knowledge and experience of domestic and foreign secret services, public institutions, as well as

the achievements of scientific research centres in the field of terrorism prevention. It intends to develop a broad preventive mechanism based on the cooperation of all public administrative bodies and the private sector, placing citizens in the centre of the process of shaping security culture in Poland. To achieve such objectives, the Centre develops training programmes and conducts training in the field of terrorism prevention. A significant part of the Centre's activities are social campaigns that raise awareness of terrorist threats and build security culture within the society. The Centre also prepares profiled recommendations in the field of terrorism prevention and develops training materials and guides. It has also been involved in the organisation of meetings, workshops, and seminars both at the national level and in cooperation with domestic and foreign experts.

Although the Centre is a relatively new institution, it has successfully combined national and foreign experience and expanded its capacities and staff. As at September 2020, the Centre has been involved in 17 state-wide projects, cooperating with 40 partners, organising 300 meetings and providing training to 3,841 persons within a broader system of prevention to terrorism and extremism (Terrorism Prevention Centre of Excellence, 2020).

The terrorist threat will remain an important issue for Poland's internal security for years to come. Although there have been no terrorist attacks in Poland in recent years, jihadist terrorist networks have operated there, planning and supporting attacks in other countries. There is a growing concern of rising extremism, typically extreme and nationalist right wing and neo-Nazi affiliated networks that call for violence against ethnic and social minorities. Such networks may increase cooperation with similar organisations from abroad and shift from non-lethal violence to more coordinated attacks with firearms and explosives. They will be susceptible to external influence and might be used as a tool in hybrid activities in Poland and abroad. Most likely, at least some of the extremist networks will also engage in criminal activities. The potential for lone wolves as perpetrators of terrorist attacks and hate crimes must also be taken into account when discussing future developments related to Poland's internal security (Raubo, 2020).

3. THREATS TO THE SECURITY OF POLAND'S CYBERSPACE

Similar to other states, Poland is becoming more and more dependent on cyberspace-enabled services. Social and economic development is increasingly dependent on quick and unhindered access to information. The efficiency and stability of ICT systems are crucial not only for the internal security of the state but also have an impact on virtually every area of state and civil activity. The period between 2015 and 2020 saw an evolution of cyber threats that had a direct impact on Poland's internal security. The Internal Security Agency's CSIRT GOV team reacted to more than one hundred thousand computer incidents between 2015 and 2019. One-third of those incidents turned out to be cyber threats. The number of computer incidents has steadily increased after 2015. Whereas in 2015 CSIRT GOV dealt with 16,123 cases of suspected computer incidents, the number of such cases rose to 31,865 in 2018 and 226,914 in 2019 (Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego, 2019). Most of the cases turned out to be false positives and the numbers of confirmed computer incidents were 8,914 in 2015, 6,236 in 2018, and 12,405 in 2019. Advanced persistent groups campaigns have constituted a growing portion of the threats to Poland's cyberspace after 2015. Most of the malicious traffic against the governmental administration networks in 2019 originated from the Russian cyberspace. Communication to malicious internet addresses along with active scanning of the governmental administration networks made up almost 80% alerts issued by the early warning systems. Government institutions (32.81%), critical infrastructure (31.21%), and the Ministries (19.01%) were most frequently subjected to active scanning in 2019. State security services and military accounted for only 5.27% of active scanning cases in 2019 (Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego 2017, 2018, 2019).

The urgency of actions to assure Poland's cybersecurity was recognised as early as in 2015. The Supreme Audit Office reports published at the time pointed at critical deficiencies in defining the legal and conceptual framework for actions, deficient financing and insufficient coordination (Najwyższa Izba Kontroli, 2015). The security of state administration infrastructure used for public services was determined to be inadequate

by the Supreme Audit Office in 2016 (Najwyższa Izba Kontroli, 2016). Similar audits of the local government administration infrastructure in 2018 revealed shortcomings in data protection systems (Najwyższa Izba Kontroli, 2019). The situation called for a coordinated and comprehensive approach to the security of Poland's cyberspace. In 2018, the Act on the National Cybersecurity System was finally adopted after lengthy preparations, and in 2019, the Strategy for the Protection of the Cyberspace of the Republic of Poland for 2019–2024 was published (Ministerstwo Cyfryzacji, 2019). A decade after initial governmental efforts related to cyberspace security, a coherent legal and conceptual framework for action has been finally developed. While not all issues have been resolved, a solid basis for further works has been established (Cieślak, 2020).

Cybersecurity has remained one of the key areas for the Internal Security Agency in recent years. The operations of CSIRT GOV have focused on the protection of the state's administration cyberspace. The CSIRT GOV Computer Security Incident Response Team, led by the Head of the Internal Security Agency, acts as the national level CSIRT responsible for coordinating the process of responding to computer incidents occurring in the national cybersecurity system (Polska, 2018). It is tasked with the detection and prevention of threats to the cyber security of ICT systems of public administrative bodies. The CSIRT GOV also protects the system of ICT networks covered by a uniform list of facilities, installations, devices, and services included in the critical infrastructure, as well as ICT systems, owners, and holders of critical infrastructure facilities, installations or devices, defined in legal regulations on crisis management. As the number of threats and security incidents has been increasing in recent years, each incident has been addressed as a risk of violating the security of the state and citizens.

In order to ensure a more efficient response to any threats to Poland's cybersecurity, CSIRT GOV has been expanding its early warning systems and participation in international cybersecurity networks. The ARAKIS 3.0 GOV early warning system provides data on both external threats and vulnerabilities of the state's administration information and computer networks. It has been extensively used for testing vulnerabilities. In 2019, CSIRT GOV audited 35 information and computer systems of ten government administrative institutions, revealing 13,035 vulnerabilities. Corrective actions have subsequently been undertaken. Important

political events, such as elections to the European Parliament and Poland's Parliament, along with official national holidays and anniversaries, have been considered as high-risk events in terms of cybersecurity. Due attention is paid to the monitoring and mitigation of cyber threats related to such occasions. Polish CSIRT teams have systematically participated in multinational exercises, such as NATO-CMX, Cyber Coalition, and Locked Shields to prepare better for the protection of the state's cyberspace (Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego 2019).

The security of Poland's cyberspace will remain crucial for the state's internal security. As the dependence on network-enabled services is ever-increasing, the need for a comprehensive approach to the cybersecurity system becomes more and more urgent. Poland will have to increase its efforts to improve the protection of the critical infrastructure assets (Rządowe Centrum Bezpieczeństwa, 2020). Better private-public partnership solutions in the field of cybersecurity have been sought for, and significant efforts are directed at improving Poland's independence in the digital domain through the development of cryptographic tools and national expert cyber centres. The need for a secure cyberspace becomes even more evident as it is used more and more frequently for hostile information operations and hybrid activities.

4. THREATS TO ECONOMIC SECURITY

The National Security Strategy of the Republic of Poland published in May 2020 recognised the urgency of strengthening economic security being faced by globalisation processes and growing competition on foreign markets. This is directly linked with internal security, national defence potential but also with state and societal resilience in the face of modern threats. Special attention has been given to the financial sector, which is vulnerable to speculative attacks on the Polish currency or capital drain. As this sector is significantly affected by external trends, there is a need to close ranks with international supervisory institutions and internal law enforcement agencies. Financial stability is an essential factor motivating the use of the Polish banking system for money laundering, as it has been in the case of the ING Bank Śląski, a subsidiary of the ING BSK, which was used to launder Ukrainian and Russian money within a so-called 'mirror trading' system. Another bank, Bank Spółdzielczy in Skierniewice, was the subject of a prosecutors' investigation connected to money laundering and drug trade; deposits valued at 1.3 bn PLN were seized (Wilkowicz, 2020). Those are not only cases, and their impact is important from the perspective of trust in the national banking system and overall security, as financial issues are of great importance for every citizen. From another vital perspective, the financial sector is closely connected to the position of a country in the international arena. Therefore, reasonable and purposeful government interference in economic matters is an essential factor for the security in this sector after 2015.

Another factor affecting the internal security of Poland is the safety of the supply of natural resources. Oil and natural gas have been traditionally exploited by Russia as an international policy tool to pressure selected nations. This is done directly by establishing different prices for different nations, specifically those recognised as hostile or friendly. After decades of a Russian monopoly in supplying oil and natural gas to Poland, a common perception of threats resulting from such a situation has developed. Poland is clearly aware of such threats, demonstrated by the investment in a strategically important Liquid Natural Gas Terminal in Świnoujście to ensure the stability of supplies for the population and state enterprises. The termination of gas supplies to Ukraine by Gazprom in the recent past

has demonstrated the effect of such a tool on economic and personal security. In parallel, Warsaw is actively trying to stop the Nord Stream 2 gas pipeline project, calling it a direct threat to energy security and not only for Poland but for Eastern Europe in general. The decision of the Office of Competition and Consumer Protection in October 2020 to impose a penalty on Gazprom (29bn PLN) and five companies participating in the project (234mln PLN) was a clear message and an act of protecting national economic interests (U.N. Security Council Counter-Terrorism Committee, 2019). This aspect is linked with gas prices and continuity of supplies as increasing prices on the internal market could cause dissatisfaction among natural gas users in Poland, especially among the poorer part of society and strategic companies using this type of natural resources for production processes. At the same time, the Internal Security Agency has been focusing its efforts on protecting the Liquid Natural Gas Terminal project in Świnoujście against hostile economic and information actions.

Poland's state security services have become increasingly aware of hostile economic and financial actions that may directly influence the state's internal security. In 2015, the Russian fertiliser tycoon Acron was trying to take over Polish chemicals giant Grupa Azot, which was seen as an aggressive step to monopolise the market in this specific field. In reaction, the Polish government implemented a law permitting the state control of selected national companies of strategic value. The list of such companies is evolving and includes Emitel S.A., Grupa Azoty S.A., KGHM Polska Miedź S.A, Polski Koncern Naftowy Orlen S.A, PKP Energetyka S.A., and Tauron Polska Energia S.A (Ostrowski, 2020). The government is currently working on a new law requiring foreign investors to have state approval to buy shares in a company equal or exceeding 10% share capital or concerning buying a significant block of shares (e.g. 20%, 40%).

Investors from the European Union/European Economic Area will not be subject to restrictions if they have been registered there at least two years to avoid hostile takeovers. Hostile takeover attempts are not exclusively linked with Russian capital, as, for example, KGHM falls within the area of interest of the U.S. Freeport-McMoRan Copper & Gold, Australian Rio Tinto, or Chinese investors. Next, foreign companies have taken significant interest in food production companies, which is an important factor that could influence the food prices in Poland and affect food security

along with the protection of natural environment. It might affect the basic needs of the population with a strong influence on societal stability. The trend to take over Polish companies is growing, and it is linked to the Covid-19 crisis and weakness of the currency and the continuing expansion of big and rich players. There are direct risks connected to this factor, as taxes from national enterprises support the Polish economy, while in the case of companies funded by foreign capital, the funds are transferred abroad.

The economic sphere has always been attractive for crime-related activities, especially tax violations and corruption among participants on both ends – givers and receivers. The crime-supporting factor in Poland is that it has been benefiting from significant economic growth during the last decades using national resources along with significant funds coming from the EU. Investments into infrastructure are creating opportunities at all levels and stages of their implementation. The Poland Corruption Report published in January 2018 highlighted that corruption was a problem for businesses operating in Poland (GAN Risk & Compliance Portal, 2018). The public procurement, justice, and land administration sectors carry exceptionally high risks. Political corruption constitutes a challenge to fair business as politicians use their positions to gain benefits, and practices of nepotism and cronyism are widespread. Poland's Criminal Code offences include active and passive bribery, bribery of foreign officials, extortion, and money laundering. The public procurement sector was especially linked with this negative trend by a diversion of public funds and favouritism in decisions of government officials, tailor-made specifications for particular companies, unclear selection or evaluation criteria, collusive bidding, and conflicts of interest (GAN Risk & Compliance Portal, 2018). However, the Corruption Perceptions Index (CPI) indicates that Poland has made progress in this area: the Transparency International CPI 2019 ranked Poland 41st with 58 points (the scale: highly corrupted 0 points, minimal corruption 100 points). This is a result of a decisive approach toward fighting this negative aspect of the economy having an impact on nations and other factors as Foreign Direct Investments.

The Internal Security Agency can also boast considerable successes in combating economic crimes. According to one study, the Internal Security Agency has revealed attempts at tax fraud for over PLN 3 billion

and conducts, under the supervision of various units of the prosecutor's office, an average of 140 proceedings concerning tax offences each year. Some 1.5 thousand persons received accusations of committing tax crimes, and the value of the secured property of suspects in tax depletion cases is over PLN 260 million (60 mln Euro) (Serwis Rzeczypospolitej Polskiej, 2020a). The negative trend is, however, that corruption cases are more common in the public sector compared to private or public/private sectors. In 2018, of a total of 1,229 cases, 895 were in the public sector (73%), and the trend continued in 2019 as among 1,366 corruption cases as many as 948 (70%) were related to the public sector (Internal Security Agency, 2020). The main areas of corruption were infrastructure, construction, and real estate. The trend is reinforced by the employment of random people in the public sector not able to manage and control respective enterprises. It is often linked with nepotism and returning favours to trusted persons but not exactly qualified ones.

The economy-related threats and risks are highly interconnected, as many of them have an impact on security from the national level down to single individual personal security. Therefore, there is a need to see all of them in context, not forgetting that the country is a part of broader international systems as an outcome of globalisation and a variety of agreement. As mentioned, the banking system, natural resources supplies, and others are under pressure from external competitors or hostile nations/organisations reinforced by internal risks line crimes, corruption, nepotism or politically driven economic system. The Internal Security Agency will continue to play an important role in addressing external economic threats to Poland's security.

CONCLUSIONS

The internal security of Poland has been subject to a number of external threats in recent years. Russian aggressive actions have destabilised the security situation in the Euro-Atlantic area and increased the scope and magnitude of threats to Poland's external and internal security. Poland has been facing a growing threat of foreign espionage, intelligence, and influence operations. While most of them are attributed to the Russian Federation, the intensity of Chinese secret services actions in Poland raises more and more concerns. Terrorism and extremism have not resulted in a high number of casualties or losses in recent years, and the overall terrorist threat has remained relatively low. However, terrorism and lone wolf attacks motivated by extremist narratives and ideas may pose a threat to Poland's internal security in coming years.

Hybrid threats have become one of the critical threats to Poland's internal security and are considered to be tied closely to the actions of adversary governments. The recent years have seen a blurring of the boundaries between intelligence threats and hostile cyber, terrorist, and economic activities carried out inside Poland and outside of its borders. Propaganda and disinformation inspired by Russia have become the primary instruments of hybrid activities carried out in cyberspace. They weaken Poland's security and its position in international relations. At the same time, hybrid activities exploit political divisions and extremisms among Polish citizens, undermining the internal security of the state and its resilience to external threats.

The trends that have been observed in recent years suggest that the scope and magnitude of cyber threats to Poland's security will grow significantly in the coming years. Actions of foreign states, along with criminals, will pose a threat to Poland's public administration, industry, and banking, as well as individual citizens. Furthermore, the cyberspace may be used for hybrid activities and hostile information operations. The protection of Poland's cyberspace will remain crucial for the state's internal security in the coming years. A comprehensive approach combining public and private efforts will focus on the improvement of the protection of the critical infrastructure assets. Actions aimed at Poland's independence

in the digital domain will be given priority. That, in turn, will translate into more robust efforts related to the development of cryptographic tools and building national cyber expertise.

Protection of Polish economic interests against external hostile activities will remain one of the primary tasks of the Internal Security Agency in the future. The economy has a direct impact on internal security both at the national level and for the security of any individual citizen. With the globalisation of the economy, the frequency of potential external state and commercial actors' interference with the Polish economy may increase, and their intentions may not always be clear. The protection of vital national investments against hostile takeovers, corruption, and hybrid activities will be given priority as such investments improved Poland's security. The actions of the Internal Security Agency will be coordinated with other state's security agencies, as well as the Central Bureau for Anticorruption and the Police.

REMARK

The views presented by the authors are their own opinions and do not represent the official position of the Baltic Defence College.

Contacts:

Eugeniusz Cieślak, PhD
Baltic Defence College
E-mail: Eugeniusz.cieslak@baltdefcol.org

Zdzisław Śliwa, PhD
Baltic Defence College
E-mail: Zdzislaw.sliwa@baltdefcol.org

REFERENCES AND SOURCES

Cieślak E., (2020). Adressing the threats to national security. Poland's experience. In: Bekesiene S. and Hoskova-Mayerova S., *Challenges to national defence in contemporary geopolitical situation. CNDCG' 2020 Proceedings of the 2nd International Scientific Conference. Vilnius, Lithuania.* Vilnius: LKA

Deutsche Welle., (2018). *Poland busts Russian 'hybrid warfare' ring.* [Viewed 8 September 2020]. Available from: https://www.dw.com/en/poland-busts-russian-hybrid-warfare-ring/a-43831566

Forsal., (2019). *Raport ABW: Najpoważniejsze wyzwania w sferze bezpieczeństwa wiążą się z agresywną polityką Rosji*, 6 grudnia. [Viewed 15 September 2020]. Available from: https://forsal.pl/artykuly/1443411,abw-najpowazniejsze-wyzwania-w-sferze-bezpieczenstwa-wiaza-sie-z-agresywna-polityka-rosji.html

GAN Risk & Compliance Portal (2018), *Poland Corruption Report.* [Viewed 4 October 2020]. Available from: https://www.ganintegrity.com/portal/country-profiles/poland/

Infosecurity 24., (2020). ABW zatrzymała obywatela Niemiec podejrzewanego o udział w grupie o charakterze terrorystycznym. *Inforsecurity24.pl*, 1.10. [Viewed 8 October 2020]. Available from: https://www.infosecurity24.pl/abw-zatrzymala-obywatela-niemiec-podejrzewanego-o-udzial-w-grupie-o-charakterze-terrorystycznym

Lesiecki R., (2019). Polska definicja szpiegostwa do zmiany. Szef speckomisji dla *InfoSecurity24.pl*, 16.01. [Viewed 8 October 2020]. Available from: https://www.infosecurity24.pl/polska-definicja-szpiegostwa-do-zmiany-szef-speckomisji-dla-infosecurity24pl

Maciążek P., (2019). *Gdzie się podziały jawne raporty ABW?*, 03.12 [Viewed 8 October 2020]. Available from: https://osluzbach.pl/2019/03/12/maciazek-gdzie-sie-podzialy-jawne-raporty-abw/

Ministerstwo Cyfryzacji., (2019). *Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024.* [Viewed 26 September 2020]. Available from: http://prawo.sejm.gov.pl/isap.nsf/ DocDetails.xsp?id=WMP20190001037

Mölder, H. (2016). The War of Narratives – Putin's Challenge to International Security Governance in Ukraine. *Estonian Journal of Military Studies*, VI (2)

Najwyższa Izba Kontroli., (2015). *Realizacja przez podmioty państwowe zadań w zakresie ochrony cyberprzestrzeni RP. Informacja o wynikach Kontroli. KPB-4101-002-00/2014 Nr ewid. 42/2015/p/14/043/KPB.* [State authorities'

fulfillment of tasks related to protection of the Republic of Poland's cyberspace. The information of the control results]. [Viewed 26 September 2020]. Available from: https://www.nik.gov.pl/plik/id,8764,vp,10895.pdf

Najwyższa Izba Kontroli., (2016). *Zapewnienie bezpieczeństwa działania systemów informatycznych wykorzystywanych do realizacji zadań publicznych*, KPB.410.004.05.2015, Nr ewid. 42/2016/p/15/042/KPB. [Ensuring the operational security of IT systems used to carry out public tasks]. [Viewed 26 September 2020]. Available from: https://www.nik.gov.pl/plik/id,10771,vp,13104.pdf

Najwyższa Izba Kontroli., (2019). *Zarządzanie bezpieczeństwem informacji w jednostkach samorządu terytorialnego*, [Information security management in local self-government administration entities]. [Viewed 26 September 2020]. Available from: https://www.nik.gov.pl/kontrole/wyniki-kontroli-nik/pobierz,kap~p_18_006_201807261245431532609143~01,typ,kk.pdf

Internal Security Agency, (2020), *Obszary przestępczości korupcyjnej w Polsce w latach 2018–2019*, Internal Security Agency, Warsaw.

Ostrowski S., (2020). Ochrona polskich spółek przed przejęciami. Jak nowe prawo ma działać w praktyce?. *Forsal.pl* 2 June. [Viewed 8 October 2020]. Available from: https://forsal.pl/artykuly/1480601,ochrona-polskich-spolek-przed-przejeciami-jak-nowe-prawo-ma-dzialac-w-praktyce.html

Poland., (2020). *National Security Strategy of the Republic of Poland*. [Viewed 22 September 2020]. Available from: https://www.bbn.gov.pl/ftp/dokumenty/National_Security_Strategy_of_the_Republic_of_Poland_2020.pdf

Polska. *Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa*. Warszawa. Kancelaria Sejmu. [Viewed 26 September 2020]. Available from: http://prawo.sejm.gov.pl/isap.nsf/download.xsp/ WDU20180001560/U/D20181560Lj.pdf

Raubo J., (2020). Pracowity rok polskich służb specjalnych [OPINIA], 6 stycznia. [Viewed 8 October 2020]. Available from: https://www.infosecurity24.pl/pracowity-rok-polskich-sluzb-specjalnych-opinia

Rządowe Centrum Bezpieczeństwa, (2020). *Narodowy Program Ochrony Infrastruktury Krytycznej – tekst jednolity. Uchwała nr 210/2015 Rady Ministrów z dnia 2 listopada 2015 r. w sprawie przyjęcia Narodowego Programu Ochrony Infrastruktury Krytycznej z uwzględnieniem Uchwały nr 116/2020 Rady Ministrów z dnia 13 sierpnia 2020 r. zmieniającej uchwałę w sprawie przyjęcia Narodowego Programu Ochrony Infrastruktury Krytycznej*. [Viewed 10 October 2020]. Available from: https://rcb.gov.pl/wp-content/uploads/Narodowy-Program-Ochrony-Infrastruktury-Krytycznej-2020-tekst-jednolity.pdf

Sazonov V. and Müür K., (2017), Introduction: Russian Hybrid and Information Warfare, in Sazonov V. et al (eds) *Russian Information Operations Against Ukrainian Armed Forces and Ukrainian Countermeasures (2014–2015),* ENDC Occasional Papers No 6/2017, pp. 9–12

Serwis Rzeczypospolitej Polskiej, 2020. *Podsumowanie działań ABW.* [Viewed 26 September 2020]. Available from: https://www.gov.pl/web/sluzby-specjalne/podsumowanie-dzialan-abw

Serwis Rzeczypospolitej Polskiej, 2020. *Silny kontrwywiad, silne gwarancje bezpieczeństwa.* [Viewed 21 September 2020]. Available from: https://www.gov.pl/web/sluzby-specjalne/silny-kontrwywiad-silne-gwarancje

Śliwa Z., (2017), "Hybrid Warfare" – The Military Security Domain's Considerations in Sazonov V. et al (eds) *Russian Information Operations Against Ukrainian Armed Forces and Ukrainian Countermeasures (2014–2015),* ENDC Occasional Papers No 6/2017, pp.13-27

Terrorism Prevention Centre of Excellence., (2020). *Centrum Prewencji Terrorystycznej to jednostka Agencji Bezpieczeństwa Wewnętrznego zajmująca się w szeroko pojętą profilaktyką antyterrorystyczną.* [Viewed 26 September 2020]. Available from: https://tpcoe.gov.pl/cpt/o-nas/1659,Centrum-Prewencji-Terrorystycznej-to-jednostka-Agencji-Bezpieczenstwa-Wewnetrzne.html

UN Security Council Counter – Terrorism Committee, 2019. *CTC conducts its first assessment visit to Poland.* [Viewed 28 September 2020]. Available from: https://www.un.org/sc/ctc/news/2019/12/17/ctc-conducts-first-assessment-visit-poland/

UOKiK, (2020). *Nord Stream 2 - maximum penalties imposed by UOKiK President.* [Viewed 25 September 2020]. Available from: https://www.uokik.gov.pl/news.php?news_id=16818

Wilkowicz Ł. (2020). 'Polska nie jest już bezpieczną przystanią. Chodzi o pranie pieniędzy' [online]. *Dziennik.pl.* 22 September. [Viewed 3 October 2020]. Available from: https://gospodarka.dziennik.pl/news/artykuly/7829060,polska-bezpieczna-przystan-pranie-pieniedzy-banki-knf-aml.html

Winnerstig, M. (2014). *Tools of destabilisation: Russian soft power and non-military influence in the Baltic States.* FOI-R-2990-SE. [Viewed 5 October 2020]. Available from: https://www.stratcomcoe.org/mike-winnerstig-ed-tools-destabilization-russian-soft-power-and-non-military-influence-baltic-states

Żaryn S., (2019). NATO 2020 Defined. Poland's Internal Security Service is critical to hunting down spies. *Defense News* December 2. [Viewed 8 October 2020]. Available from: https://www.defensenews.com/opinion/

commentary/2019/12/02/polands-internal-security-service-is-critical-to-hunting-down-spies/

Żaryn S., (2019). *Russia's hybrid warfare toolkit has more to offer than propaganda*, August 09. [Viewed 3 October 2020]. Available from: https://www.defensenews.com/opinion/commentary/2019/08/09/russias-hybrid-warfare-toolkit-has-more-to-offer-than-propaganda/

Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego (CSIRT GOV)., (2020). *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2019 roku.* [Viewed 5 October 2020]. Available from: https://csirt.gov.pl/cer/publikacje/raporty-o-stanie-bezpi/969,Raport-o-stanie-bezpieczenstwa-cyberprzestrzeni-RP-w-2019-roku.html

Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego (CSIRT GOV)., (2019). *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2018 roku.* [Viewed 5 October 2020]. Available from: https://csirt.gov.pl/cer/publikacje/raporty-o-stanie-bezpi/964,Raport-o-stanie-bezpieczenstwa-cyberprzestrzeni-RP-w-2018-roku.html

Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego (CSIRT GOV)., (2017). *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2016 roku.* [Viewed 5 October 2020]. Available from: https://csirt.gov.pl/cer/publikacje/raporty-o-stanie-bezpi/957,Raport-o-stanie-bezpieczenstwa-cyberprzestrzeni-RP-w-2016-roku.html

COMPETING STRATEGIC NARRATIVES AND THEIR REFLECTIONS IN PRACTICE: RUSSO-ESTONIAN RELATIONS FOLLOWING THE ANNEXATION OF THE CRIMEA

Viljar Veebel, PhD
Baltic Defence College
Department of Strategic Studies
Researcher

Raul Markus, M.A.
Tallinn University of Technology
School of Engineering
Department of Mechanical and Industrial Engineering
PhD student

Liia Vihmand, M.A
Tartu University
College of Foreign Languages and Cultures
PhD student

Keywords: strategic narrative, security, concerns, trade, Russia, Estonia

ABSTRACT

The current article analyses the prospects of improvement in terms of economic and political relations between Estonia and Russia against the inert background of reciprocal strategic narratives. Estonia's current strategic narrative regarding Russia is mostly influenced by the country's painful historic experience, plus the continuing social segregation within the country between Estonians and Russians, and security threats that stemming from Russia and requiring active NATO deterrence. Russia's domestic vision includes 'Russophobic' western enemies, including Estonia, which surround and threaten it and which place it under an economic blockade. Both sides are also locked into a greater framework involving the European Union's economic sanctions against Russia and Russian counter sanctions. On the other hand, both Estonia and Russia have a lot to gain from possible improvements in economic relations and in reducing regional security-related tensions.

INTRODUCTION

Estonia, along with the other Baltic States, is experiencing a series of deep transformations that can be associated with the drastic deterioration of Europe's relations with Russia in the aftermath of the annexation of the Crimea and the Russia-inspired conflict in eastern Ukraine. However, the ongoing transfiguration of the liberal order lacks one single point of logic and encompasses a number of politically consequential developments that directly affect the Baltic States. There are several facets involved in this situation, the first being the EU-promoted normative space of liberal governance and normative power. The second is the Russo-German bilateral 'economic regionalism' that has been exemplified by the Nord Stream project and the prioritisation of economic relations. The third is the resurgent domain of the regional security complex in the Baltic States, along with the dominant logic of providing a military deterrence and the process of ramping up security levels.

These facets often confront each other and make improvements to regional security and trade somewhat complicated. However, during the recent visit by the president of Estonia, Ms Kersti Kaljulaid, to Russia in April 2019, there was a good deal of discussion about the strengthening of economic relations between the two countries. To quote President Kaljulaid, although mutual sanctions between Russia and the EU are in place, there are some areas in which Tallinn and Moscow could cooperate and move forward, such as transport and taxation (ERR, 2019a). This appears to indicate that Estonia is interested in tightening economic relations with Russia (see ERR, 2019b, for instance where proof is needed). However, just a few months earlier the then-Estonian Minister of Foreign Affairs, Sven Mikser, firmly underlined the fact that relations between Estonia and Russia depended primarily upon Russia's behaviour in the international arena in the sense that Russia neither fulfils its obligations nor accepts international law. In this light, bilateral relations between Estonia and Russia simply cannot bloom, regardless of any other aspects. Furthermore, he argued that, based on the historical experience, Estonia sees its role as a country that needs to remind other democratic countries of Russia's unacceptable behaviour (Veebel, 2018). Therefore, within a short period of time, two high-level office-holders in Estonia have sent

considerably mixed signals regarding Estonia's vision of how mutual relations between two countries should develop in the future.

This article aims to discuss the options for providing any improvement to economic and political relations between Estonia and Russia against the background of reciprocal strategic narratives. In general, the outlook for economic relations could be approached in many ways, such as by evaluating the impact of terms of trade or various policy measures which could include economic sanctions, and so on. However, the focus of this study remains fixed on national strategic narratives because, in the interpretation of the authors, strategic narratives reflect policy goals which guide decision-making (De Graaf *et al,* 2015). Next to that, the article discusses the future outlook of economic relations between Russia and the Baltic countries in the wider perspective, referring to a structural transition from a liberal to a post-liberal international order. The process clearly encompasses a number of politically sensitive developments that directly affect the Baltic region.

1. IS THE PROCESS OF RAMPING UP BALTIC SECURITY LEVELS BEING OVERDONE?

This article sees as the relevant theoretical basis for understanding the inner structure and construction process of the narratives being discussed in terms of the process of ramping up the theory regarding security levels. The authors see this as providing common ground, whereby both Estonian and Russian narratives could be brought together and analysed in detail. As will be argued, both narratives can be seen as interpreting a mutual past, present, and future in clear ideological terms and, thereby, strongly influencing the respective reality. Drawing on Buzan's works and his direct contribution, the concept of the process of ramping up security levels has also been developed by the members of what came to be known as the Copenhagen School, with such members as Ole Wæver, Jaap de Wilde, Thierry Balzacq, and others. The end of the Cold War opened up an intensification of debates regarding the referent objects of security: security increasingly drifted away from a purely statistical concept and towards a meaning that involved the security of the state and a view of security as that of the individual. Through the implementation of these incentives, the theory behind the process of ramping up security levels is directly linked to a comprehensive approach to national defence, as this differentiates between various sectors (such as military, political, economic, societal, and environmental sectors), and specific threats that are attributable to each and every sector. This approach makes it clear that existential threats are actually subjective, referring to the contextual nature both of security and security threats (Eroukhmanoff, 2018).

The mechanisms behind the theory regarding the process of ramping up security levels were summed up well by various people, such as, for example, Rita Taureck, who asserted that 'by stating that a particular reference object is threatened in terms of its existence, a player in the process of increasing security levels claims a right to extraordinary measures to ensure the reference object's survival. The issue is then moved out of the sphere of normal politics and into that of emergency politics, where it can be dealt with outside of the normal rules and regulations of policy making. For security purposes, this means that it no longer has any given (pre-existing) meaning but that it can be anything that

a player in the process of increasing security levels says it is' (Taureck, 2006, p 3). In this way, security is the act of speech through which security itself is constructed (Wæver, 1995, pp 55–56), a discursive practice which adds the label of security to any issues that are considered to be of supreme priority and, thereby, legitimises a player's claim to apply extraordinary measures (Buzan *et al,* 1998, p 26). The process is successful when a target audience accepts such a construction and supports extraordinary measures to address the threats (Buzan *et al,* 1998, p 34). As will be argued, the Estonian take on the comprehensive approach and on resilience along the lines of total defence brings along a tendency to impinge the security aspect upon a layer of questions that are related to civil society and to see it as a mere support mechanism for the purposes of defence. However, it removes these issues from the ordinary political debate. Here, Wæver's theory regarding the process of ramping up security levels allows this phenomenon to be critically examined. It makes it possible to see that a comprehensive approach to security has a built-in tendency to add the security aspect to the entire spectrum of public policies, subsuming them under the heading of comprehensive security. Several authors have stated that, in this way, the theory behind the process of ramping up security levels shifts the focus of security studies to the intersubjective level: 'security is a social and intersubjective construction' (Taureck, 2006), 'threats are not separable from the intersubjective representations in which communities come to know them' (Balzacq, 2011, p 214), 'there is no distinction being made between a "real threat" and a "perceived threat", there is only an intersubjective understanding of a threat' (Hjalmarsson, 2013, p 3), to quote some of them. The foundations of theoretical studies by Barry Buzan and the Copenhagen School are also to be found in the practice of international relations. Accordingly, the authors of this study aimed at illustrating the fact that the first stepping stones of a comprehensive approach to security can be found in the growing realisation through international practice of the holistic nature of security, including military, diplomatic, statehood, human security, environmental aspects, and social aspects.

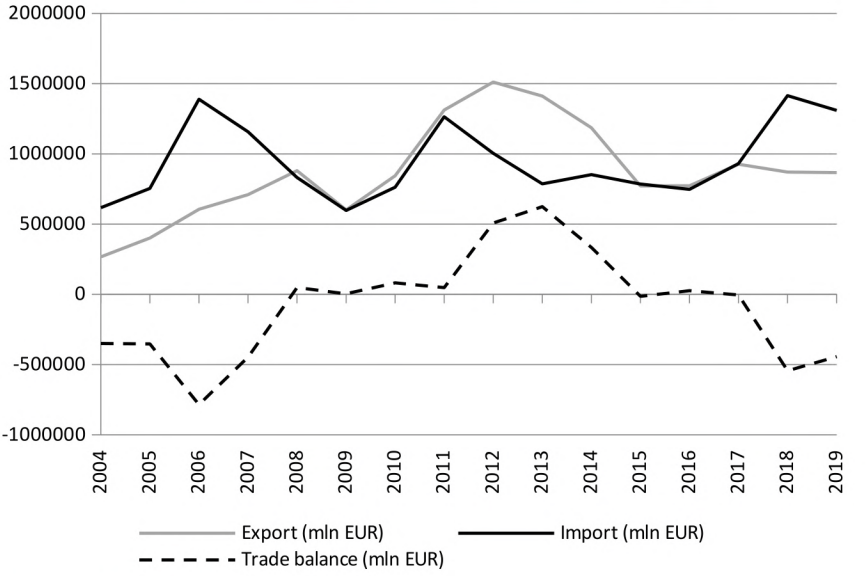
Next to the primary interest point for this article as part of the prospect of a normalisation of economic relations between Estonia and Russia, it is interesting to note that the narratives have another aspect in regard to the democratic character of the state, especially for Estonia. This largely relates to the ramping up of security levels in relation to economic

relations which could be seen as yet another layer in the logic of total defence whereby an entire field is taken out of its normal liberal domain and is pigeon-holed into a corporate logic of clearly-dominant national interests prevailing over economic or civilian interests. Although there appear to be good grounds for mutual distrust, Estonia especially should be aware that it could lead to the state being transformed into a corporate body that is oblivious of its requirements to take care of its population. In more detail, the danger exists that while relying too heavily upon such a narrative, one switches into a war mode. Due to the character of modern hybrid warfare becoming ever more permanent, Estonia could easily find itself in a situation in which the low-intensity hybrid context transforms its normal *modus vivendi* into a wartime total defence mode of existence (Veebel and Ploom, 2019).

2. ECONOMIC RELATIONS BETWEEN RUSSIA AND ESTONIA OVER THE PAST DECADES

Over the past fifteen years, trade relations between Estonia and Russia have faced turbulent times (see Figure 1). A boom in trade relations in 2004–2006 after Estonia's accession to the EU was followed by a 'bust' period in 2007–2009 due to strained mutual relations and the global economic crisis. Trade between the two countries intensified again in 2010–2012 as a result of the economic recovery of the region after the global economic crisis. However, from 2012 onwards, trade flows have stagnated significantly. Only recently, since 2016, have trade flows between Estonia and Russia started to increase again (see Veebel and Markus, 2018).

FIGURE 1: Estonia's imports and exports with Russia in 2004–2019 (in EUR).



Source: Statistics Estonia, 2019.

Next to changes in economic conditions, the dynamics of bilateral trade flows between Estonia and Russia in the recent past have often been

affected by changes in political relations. For example, the setback in trade relations in 2007–2009 was partially caused by Russia's retaliatory attempt to destabilise Estonia's economy, referring to the conflict over what was known as Estonia's Bronze Soldier monument in Tallinn. During the conflict in April 2007, Russia also called for a cessation of diplomatic relations with Estonia. This was coupled with large-scale cyber-attacks against Estonian state institutions, the blockade of the Estonian embassy in Moscow by Russian youth movements, calls for a boycott by Russian officials against Estonian products, the blocking of goods vehicle traffic at the main connecting bridge into Estonia, and the cutting-off of the delivery of oil, coal, and petroleum products into Estonia (Roth, 2009). These actions have increased the cautiousness of Estonian entrepreneurs as far as deepening economic relations with Russia are concerned. Furthermore, in 2012–2014, Russia implemented several measures to protect its local producers, despite Russia's WTO membership. For example, the importation of live animals and dairy products was banned and several sanctions were introduced in relation to the Estonian fishing sector. This has even further decreased the incentive of Estonian entrepreneurs to enhance trade relations with Russia. Last but not least, mutual sanctions between the EU and Russia which were imposed during the Ukrainian conflict from 2014 onwards have also left their mark on economic relations between Estonia and Russia. Although the overall impact of the Russian sanctions on the economic growth of the EU has been estimated to be rather limited, according to estimations (such as those by Mauricas, 2015; Oja, 2015), the Baltic countries were amongst the EU states to be most heavily affected by Russian sanctions. Russian sanctions have seriously damaged some of Estonia's economic sectors, particularly the food and agricultural sectors.

The future outlook for mutual economic relations is expected to be pessimistic for the most part by Estonian policymakers and experts. Amongst many similar voices, such as, for example, Signe Ratso, the argument is that Estonian entrepreneurs should rely more on diversifying their risks and that local producers should focus on those products which have higher added value, because it certainly helps to find other markets and to request higher prices for such products. Despite the proximity of the Russian market, Estonian agricultural producers in particular should focus on other markets rather than Russia, because the latter is politically sensitive and insecure (Ratso, 2015). However, trade relations between

Russia and Estonia have been in decline on more than one occasion in the past, but have recovered after some time. This brings us back to the research question of whether economic relations between Estonia and Russia could once again recover in the aftermath of the Ukrainian conflict. The comparison of reciprocal strategic narratives and visions could give us a good hint in this regard.

3. A LOOK AT THE RESPECTIVE STRATEGIC NARRATIVE OF ESTONIA ON RUSSIA

How do we define the strategic narrative within the framework of the current study? According to Miskimmon, O'Loughlin, and Roselle (Miskimmon *et al,* 2018, p 6), strategic narratives are stories '*by which political players attempt to construct a shared meaning of the past, present, and future of international politics to shape the behaviour of domestic and international players*'. So strategic narratives may be projected to serve several aims, some of which may be very different aims, such as justifying the strategic objectives of the related states or explaining political responses to economic, political, or security crises or issues, forming international alliances, organisations and so on, and also to rally domestic public opinion.

How do the narratives originate? This internalisation of a disseminated narrative is what can be considered to be the point or origin of the narrative. For a narrative to have reasonable meaning and effect, it must be internalised by a group that forms part of the audience. Therefore, within the current study, we analyse narrative origination within the context of entrenched social identities, academic publications, and contemporary public media.

There is also a need to analyse how the narratives manage to propagate themselves. We consider the propagation of narratives as a function of the internalisation of those narratives that serve to affect attitudes that are linked to domestic and foreign political issues. We refer to these manifestations as narratives that are domestic (Estonian) and foreign (Russian in the current case). By internalising these foreign (and in some cases also hostile) narratives to the point that they crystallise into opinions about public policy, members of the population themselves legitimise and ultimately spread these foreign narrative. The degree of crystallisation and the strength of opinion creates varying degrees of vulnerability within the audience. In practice, some groups will have hardened opinions (in any direction), while others will remain more malleable and open. Segmentation analysis refines this understanding to illustrate how

combined narratives can and do resonate with, and therefore propagate through, different audience groups in Estonia.

In terms of a practical case, following the restoration of Estonia's independence in 1991, the country has constantly struggled to redefine its relationship with its biggest neighbour, Russia. On the one hand, from the 1990s onwards, Estonia's strategic narrative has mostly been grounded on the argument that it has any right at all to be a sovereign country based both on legal and historic grounds, and that Russia has in many occasions violated this right (Doroško *et al,* 2004). Next to that, the historical narrative of Estonia is characterised by the differentiation between Estonians and Russians, with both groups carrying rather clear-cut political connotations. Pääbo (2011) argues that Russians are described through a negative prism, stating that Russians have played a significant role in all of the 'big wars' that have taken place within the territory of Estonia, and that Russia has over the course of recorded history been an 'uninvited interferer', against whom Estonians have had to resist to the point of armed conflict. This view, of course, exists in parallel with an alternative, and more positive take on the matter. To highlight an example, Eerik-Niiles Kross states that nowadays, Estonians have accepted that many Russian-speaking people live in Estonia and Estonians do not feel threatened by them. However, even Kross has to admit that a degree of differentiation is still made between 'us' and 'them' (Sirp, 2015).

On the other hand, Estonia has only once had to revise its basic strategic narrative of Russia in the recent past. In the early 2000s, many international organisations (such as Nato and the EU) considered Russia as a partner and not as an adversary, which contradicted the Estonian viewpoint outlined above. For example, in the aftermath of the fall of the Berlin Wall, Nato repositioned itself from an organisation that was committed to the principle of collective defence into a multitasking body that could deal with issues beyond the initial concept of collective defence. This means that the focus of the organisation has also shifted from Russia to other topics, such as anti-terrorism activities, peace-keeping missions, and crisis management (Andžāns and Veebel, 2017). Next to that, various of the world's political leaders have expressed their widespread support for Russia. For example, in 2004, George W Bush announced that the US stood shoulder to shoulder with Russia in the fight against terrorism, and this is not a lone case. This situation was relatively confusing for Estonia

in the sense that it was unclear for Estonians how far the cooperation between the US and Russia was going to develop, and whether both countries really were fighting against the 'same enemy' or whether they may later realise that they were indeed fighting against different enemies for different purposes (for further discussion, see Made, 2004). This means that Estonia had to revise its strategic narrative towards Russia too, and had to accept that other countries may see Russia differently from the way in which Estonians saw it. The situation changed greatly following the outbreak of the Georgian war in 2008, and even more so after the beginning of the Ukrainian conflict in 2014. During the conflicts, the political leaders of Estonia had condemned Russia's actions many times, expressing their support for Georgia and Ukraine. So whereas Estonia had in the early 2000s gone along with the strategic narrative of the Western countries in describing Russia as a partner and not as an enemy, the country had to be disappointed again because this vision of Russia turned out to be not true. Therefore, it is understandable that Estonia sees its role today as a 'watchdog' among the Western countries, as someone who needs to remind democratic countries of Russia's unaccepted behaviour (see Pealinn, 2018). Yet this overlaps with the narrative of Estonia as a 'truth teller', as someone who needs to reveal to the world all the erroneous interpretations of the Second World War that Russia is constantly spreading (see Doroško *et al,* 2004).

Estonia's strategic narrative of Russia today is clearly mirrored in the public discussion and its content focuses strongly on security threats stemming from Russia. In political speeches, public discussions, Estonian-language newspapers, etc., Russia is mostly described as an adversary, or someone from whom Estonia needs to seek protection. For example, the National Security Concept of Estonia of 2017 states that immediate threats to Estonia's security are primarily related to the security situation in the Euro-Atlantic region, which, in turn, is affected by Russia's increased military activities and aggressive behaviour. The strategy document describes Russia as a source of instability due to the latter's unpredictable, aggressive, and provocative actions, such as airspace violations, offensive military exercises, and threats to use its nuclear capabilities. It also claims that Russia is interested in restoring its position as a great power, without any fear of potentially coming up against any staunch opposition with the Western world and the Euro-Atlantic collective security system (National Security Concept of Estonia, 2017).

Furthermore, the latest annual report by the Estonian Intelligence Security Service dedicates about two thirds of its volume to various threats stemming from Russia. The report sets out the following: '*the main external security threat for Estonia arises from Russia's behaviour, which undermines the international order. /…/ Ukraine will be the main target of those measures this year, but Russia will not hesitate to use them even against its ally, Belarus. /…/ Countries in the European Union and Nato are not fully protected from Russia's aggressive activities*'. The report reaches four main conclusions that directly refer to Russia's threatening behaviour. Firstly, that the Russian armed forces are consistently practising for an extensive military conflict with Nato, with all of the scenarios for Russia's command-post exercises over the last two decades having relied on the prospect of conventional warfare against Nato and its member states. Throughout this period, the structure of Russian warfare scenarios and exercises has remained the same, despite the fact that meanwhile Nato has deployed its forces in the Baltic states and Poland. Secondly, the report argues that the trigger for a military conflict between Russia and Nato will be a 'coloured revolution' in one of Russia's neighbouring countries, most likely Belarus. Thirdly, the report suggests that Estonia has to be prepared for a military incursion from the direction of Russia even if a potential conflict between Russia and Nato is sparked by events elsewhere in the world. This is probable because, as far as Russia is probably concerned, the Baltic countries constitute part of Nato that would be the easiest for Russia to attack in a time of a crisis. and also to shift the balance of military power on the Baltic Sea region in its favour. Fourthly, it states that a conflict between Nato and Russia would not be limited to military action in Eastern Europe or the Baltic countries, but would also involve Russian attacks on Western European targets, as Russian armed forces are constantly developing their doctrine of attacking 'critical enemy targets' and are building up their related medium-range weapon systems which could be used to attack targets in Western Europe (Välisluureamet, 2019).

Last but not least, the most illustrative quote that reflects upon Estonia's fears and security risks today comes from Colonel Riho Ühtegi, head of the National Defence League, who rather emotionally stated that '*The Russians can get to Tallinn in two days... Maybe. But they can't get all of Estonia in two days. They can get to Tallinn, and behind them we will cut their lines of communication and supplies and everything else. They can*

get to Tallinn in two days. But they will die in Tallinn. And they know this... They will be under fire from every corner, at every step' (see McKew, 2018). All this demonstrates that the current strategic narrative in Estonia considers Russia as an adversary. Of course, these threats are to a considerable extent real, but in terms of their construction and interpretation one can clearly detect aspects that are related to a ramping up of security.

To sum it all up, the common historical legacy with Russia takes its toll on the current ethnic composition of Estonia, its political and economic ties, and its membership in international organisations, priorities, and so on. Over the past decades, Estonia has attempted to break ties with Russia. Furthermore, the country has both systematically developed its defence forces to better safeguard its security (see for instance Andžāns and Veebel, 2017, or Cooper, 2019) as well as having contributed to the Nato Alliance with the aim of benefiting from the Alliance's deterrence model and to gain guarantees of stability and peace in the Euro-Atlantic region (Ploom, Sliwa, and Veebel, 2020). Based on the national strategic narrative, Russia clearly remains an adversary for Estonia, and other potential visions, such as 'Estonia as a bridge between East and West' or 'Estonia as a positive influencer' (i.e. someone who could encourage Russia to implement reforms and to become a democratic society) are clearly 'out of the picture' today. The lack of trust in Russia was most recently reflected in the public reaction to the announcement that the president of Estonia, Kersti Kaljulaid, visited Russia in April 2019 after many years without any high-level visits between two countries. Local politicians have mostly used either a 'wait-and-see' approach or have been critical as far as the aims of the visit were concerned and the way in which the visit was organised (see for example ERR, 2019b; ERR; 2019d). No significant results were expected in Estonia from this visit. However, in practice, this was the first high-level effort to rewrite Estonia's current strategic narrative for Russia as an enemy and to replace it with a new one, if not one in which Estonia is a bridge between East and West then at least one that involves neighbours which have the possibility of experiencing civilised cohabitation in the region.

It certainly needs a lot of time and effort for Estonians first to construct and then to accept this new narrative. However, it should not be totally impossible. A study by Doroško et al (2004) suggests that Estonia's narrative for Russia and the foreign policy Estonia is carrying out towards

Russia is not something that is inevitably negative per se, but just a practice that is being established. Indeed, the way in which Estonians see Russians is not carved in stone; however, a great deal depends upon Russia's behaviour, because Estonians expect Russia to accept international laws and democratic values. In this light, it would be unrealistic to expect attitudes to change overnight in Estonia, or that in the nearest future, Estonia could start to enhance economic contacts with Russia. However, in the long-term this certainly cannot be ruled out.

4. WHAT DOES RUSSIA THINK OF ESTONIA? A STRATEGIC NARRATIVE OF ESTONIA'S BIG NEIGHBOUR

The roots of Russia's strategic narrative in regard to Estonia can be seen to lie in the way Russia has positioned itself after the end of the Cold War in the 1990s. It has been argued that after the collapse of the Soviet Union, Russia lost two of its status symbols: its communist ideology (in contrast to the prevailing liberal democracy), and its system of so-called allies in the so-called former Soviet bloc. However, the country maintained three other status symbols: its status as the world's biggest country in terms of territory; its permanent membership on the United Nations Security Council; and its nuclear arsenal (see Made, 2004). Based on these three status symbols – size, international representation, and capabilities – Russia began to develop a new identity in the 1990s and is today exploiting those symbols in restoring its position as a great power in the world arena.

Overall, in the 1990s, Russia accepted the idea of a multipolar world with many 'power centres' (the so-called Primakov doctrine), but not the idea of a unipolar world with the US as a single power centre. Whereas the multipolar approach was considered prestigious for Russia because the country considered itself as one of these 'powers' together with the US, the EU, China, and Japan, which together effectively ruled the world, the idea of a unipolar world with the US as the supreme power was a humiliating concept for it. Intriguingly, the multipolar approach allowed Russia to emotionally realise its status symbols, but at the same time, the country clearly lacked the resources to fully realise the full potential of its multipolar image in the global arena. So in following years, Russia realised that the prospect of a true multipolar world was unrealistic because the country does not have the required resources to oppose the US. In order to avoid the resultant loss of prestige in the global arena, Russia developed an ideology of 'selective multipolarity', meaning that from time to time Russia would return to the multipolar ideology, particularly in its relations with the EU, with the aim of strengthening Russia's position in Europe in comparison to Western countries. This allows the country to demonstrate that Russia is as important as are the Western countries, at

least as far as the security environment in Europe is concerned (Made, 2004). Russia has also used the same pattern recently such as, for example, in stressing its role in 'stabilising' the Ukrainian conflict in relations with France and Germany, in guaranteeing the Minsk agreements, and in interfering in various conflict situations in other places, such as Syria and Venezuela.

In this respect, it seems to be important for Russia to demonstrate to everybody that Russia is playing an important role in the global arena. At the same time, the country very carefully selects its opponents, allies, and conflict locations. Therefore, it should not be automatically assumed that Russia is looking for conflict with everybody or that it wants them everywhere. The events in Kyrgyzstan in 2010 are a good example of that. More precisely, in 2010, the Kremlin could easily have intervened in Kyrgyzstan during the ethnic conflict when the previous government was replaced by pro-Western reformists, but Russia decided not to do so, although the government of Kyrgyzstan has asked for Russia's help in solving the violent conflict between Uzbeks and Kyrgyz. This decision is somewhat peculiar, as it would have been in the hegemonic interest of Russia to increase the legitimacy of its power in the region. Basically, the same situation happened in the 1990s, when Russia decided to send its military into southern Kyrgyzstan. However, twenty years later Russia took an opposing view and, instead of solving the conflict in Kyrgyzstan, it focused on the struggle with the US over the transit centre of Manas which is located near Bishkek, the capital of Kyrgyzstan (see Veebel, 2017).

Next to that, it has been argued that, historically, Russia's strategic narrative is closely related to the country's territorial history combined with a strong dimension of multiculturalism. In more detail, Russia's strategic narrative pays a lot of attention to unity; although, this seems to be more about territorial unity and not so much about ethnic unity (Pääbo, 2011). The protection of its territory against external pressure and invasion seems to be an important component both of Russia's strategic narrative and its domestic image. In this light, it is not surprising that today, Russia depicts the Nato Alliance as a body that threatens Russia (see Financial Times, 2016, for example). Stoicescu (2015) argues that the Kremlin's propaganda constantly accuses Western countries of provoking Russia politically and economically, interfering in Russia's internal affairs with the aim of bringing the country to its knees and toppling

Putin's administrative regime. He concludes that the main purpose of this narrative is to exploit the fear in Western countries of war, and to increase their readiness to make compromises as far as Russia's ambitions and actions are concerned (see Stoicescu, 2015).

Ethnically, Russia considers all of the ethnic groups that currently live within Russia's territory as part of Russian civilisation and culture (Pääbo, 2011). Furthermore, ethnic Russians or Russian-speaking communities in areas, such as Ukraine, Moldova, Uzbekistan, Kazakhstan, and even the Baltic countries are considered 'near abroad' regions that are within Russia's sphere of influence due to the Russian-speaking minorities that currently live there. This clearly opposes Estonia's strategic narrative which states that Estonia has the right to be a sovereign country and that Russia has on many occasions violated this right. From Russia's perspective, it has any right to protect Russian-speaking minorities in other countries. Furthermore, Russia has relied on this argument both in Ukraine and in Georgia, declaring its responsibility for the protection of the rights of certain vulnerable social segments of its neighbouring countries, and pointing out the unacceptable conditions of the Russian-speaking population in those countries (see Veebel, 2017; Schatz, 2007).

Several experts have discussed the main features of Russia's attitude towards the Baltic countries and have highlighted those problems that most trouble Russia (see Morozov, 2004; Kramer, 2003; and others). As has already been mentioned, the situation for and status of Russian minorities in the Baltic countries seems to be one of these troubling problems. High-level Russian politicians often raise this issue in the media and publicly criticise Estonia, Latvia, and Lithuania. For example, the Russian foreign minister, Sergey Lavrov has recently criticised the idea of joint schools for Russian-speaking and Estonian-speaking children, calling it unacceptable because, in his opinion, this idea is not in the best interests of the Russian-speaking minority in Estonia (Russkiy Mir, 2019).

Another problem that seems to trouble Russia is the 'truth teller' narrative of Estonia (as a country that needs to reveal to the world all the erroneous interpretations of the Second World War that Russia is constantly spreading), or the 'watchdog' narrative (Estonia as a country that needs to remind Western democracies of Russia's unaccepted behaviour). Overall, Russia prefers to call it 'Russophobic' or 'anti-Russian hysteria', referring

not only to the Baltic countries but also to the Nato Alliance and the US in general (see The embassy of..., 2018; Ellyatt, 2016, as examples). On the one hand, studies have revealed that the Russian political elite is trying to construct the identity of the 'Russian world' or 'Russkiy Mir' that is based on a positive attitude towards a joint communist past. Any attempts to oppose this narrative are considered to be attacks against the collective identity of Russia and, consequently, as a threat to Russia's security (see Tamberg, 2016, for example). Therefore, the narrative of the 'Russian world' in which countries are happy about their common communist past is completely incompatible with the narrative of Estonia as a 'truth teller'. On the other hand, Russia is constantly arguing that the prevailing opinion, particularly in Estonia and Latvia, that Russia is a threat to them is groundless, and is meant only for the purpose of solving domestic problems within the Baltic countries, such as in mobilising voters by creating the image of a foreign enemy (ERR, 2017). The situation is particularly absurd in the sense that at the same time, Russia uses the same argument to mobilise its own people by presenting the Western countries as a common enemy of Russia.

Intriguingly, Aleksandr Sõtin argues that Russia today is already used to the idea that Estonia is an independent country, and that both the Russian political elite and local diplomats think of the Baltic countries only in new terms. To describe these terms in more detail, although Nato promised not to accept these countries as members of the strategic defence alliance, it has still done so, and is currently expanding its military capabilities in the Baltic Sea region. Sõtin suggests that the fact that Russia is constantly blaming the Baltic countries for violating the rights of Russian minorities in Estonia, Latvia, and Lithuania should be considered as being part of a 'normal process' because Russia simply must justify its vision of Russophobic enemies surrounding the country. Estonia seems to be a 'secondary' country for Russia and the only aspect that makes Estonia interesting for Russia is its Nato membership. Sõtin also argues that Russia has made some miscalculations in the past as far as the Baltic countries are concerned. For example, several years ago, Russia was expecting the Baltic countries to come and beg for the restoration of transit flows, but this did not happen. Next to that, Russia was expecting that the Baltics would support the Nord Stream project, but this also failed to happen (see Piirsalu, 2018). In this light, Russia seems to picture Estonia as a 'weak' and 'unimportant' country. This

negative image of the Baltic countries is also stressed by the Russian media (Cavegn, 2017). Furthermore, some Russian media channels and policy analysts have interpreted the recent visit to Moscow by the president of Estonia, Kersti Kaljulaid, as a sign of weakness, and have argued that even those countries which initially advocated strongly for sanctions against Russia have finally realised that it is more useful to be friends and to trade with Russia (see Fefilov, 2019). This does not leave much room for cooperation on even terms between Russia and Estonia. For Russians, Russia will remain 'great and strong' and Estonia will be 'small and weak'.

5. PROSPECTS FOR MUTUAL ECONOMIC RELATIONS BETWEEN NEIGHBOURS IN THE AFTERMATH OF THE UKRAINIAN CONFLICT

As has become evident, there are fundamental differences in the national strategic narratives for Estonia and Russia, particularly in the way both countries interpret the common historical past, recognise the validity of international law, and understand their roles in the international arena. In this light, the blooming of trade relations between Estonia and Russia in the nearest future is rather unlikely because there is simply no common ground upon which to develop mutual economic contacts. It should also not be forgotten that the economic sanctions between Russia and the Western countries set limits on further economic cooperation between Estonia and Russia. Today, there seems to be no intention on the either side to lift the sanctions. On the contrary, Russia uses the narrative that sanctions are the consequence of Western hegemonic ambitions against a resurgent Russia and that countering Western sanctions is a test of Russia's ability to remain a 'great power' (see Joao, 2017). From the perspective of Western countries, EU countries simply cannot distance themselves from the European norms and values until the territorial integrity of Ukraine is restored and the conditions of the Minsk I and II agreements are fulfilled, because this would seriously harm the collective reputation of the EU as a normative power in the international arena (see Veebel and Markus, 2018). Of course, over the passing of time and with the appearance of some positive moves on behalf of Russia, the lifting of most salient sanctions could still happen. In the meantime, however, several European politicians have suggested imposing new sanctions on Russia to punish the country for the incident in November 2018, where Russia opened fire on Ukrainian vessels near Crimea (Osborn and Zverev, 2018).

Nevertheless, theoretically, the recovery of trade between Estonia and Russia is possible under certain circumstances. The first of these would involve cooperation between the EU and Russia reaching a stage that could deliver significant benefits both for Russia and Estonia. The second would be if those risks that are related to Russia's erratic behaviour on the international stage were to decrease significantly.

The first option potentially relates to the outlook for the strategic partnership between the EU and Russia. Mutual relations have long relied on the Partnership and Cooperation Agreement, which has been in force since 1997. Negotiations on the new agreement in the form of a strategic partnership were launched in 2008. In light of Russia's actions in the Crimea and in eastern Ukraine all talks on the new cooperation agreement have been suspended. In her recent visit to Moscow, the president of the Republic of Estonia, Kersti Kaljulaid, called for an upgrade of the EU-Russia cooperation programme (ERR, 2019c). The need for a 'new partnership' with Russia has also been stressed by some EU member states (such as France) within the framework of the European strategic autonomy initiative. In this sense, the new cooperation agreement between the EU and Russia may present an opportunity for Estonia to create favourable conditions in trade relations with Russia, assuming that at a certain point in time the respective negotiations will continue. Alternatively, there is most likely more motivation for both sides to cooperate after some EU-financed large-scale infrastructure projects have finally been carried out (such as the Rail Baltic railway project within the framework of the Trans-European Transport Network). Although some developments contradict this view, such as the fact that the Baltic economies are more and more services-orientated or that transit from Russia has shown historically low levels over the past two or three decades, the Rail Baltic project together with the planned tunnel between Tallinn and Helsinki are expected to allow Baltic foreign trade and transit to grow (see Veebel *et al,* 2019). This could potentially also boost economic contacts between the Baltic countries and Russia.

The second option is associated with a potential change of political regime in Russia. It could, in principle, be argued that the hidden agenda of the Western sanctions against Russia has been to initiate a regime shift in Russia without destroying the country economically. However, although more and more public protests and demonstrations have been taking place in Russia in recent years against Vladimir Putin's administration, a radical regime shift in Russia is still rather unlikely thanks to a largely missing strong and united opposition, and the lack of political alternatives.

To sum up, the normalisation of trade relations between Estonia and Russia is rather unlikely against the strategic narratives of both countries, because there is a lack of 'common ground' and motivation for both sides.

Russia is clearly able to survive and recover under veritably challenging economic conditions without developing extensive trade relations with Estonia. On the contrary, any attempt to distance itself from the current strategic narrative of Russia being surrounded by 'Russophobic' enemies would basically mean that the country gives away its main 'selling point' at the domestic level. Next to that, Russia's recent activities in destabilising its neighbouring countries clearly indicates that the country has developed a well thought-out and long-term strategy when it comes to making post-Soviet countries dependent upon Russia in various aspects, such as economic, ethnic, and military dependence, and is finally realising this advantage in achieving its political ambitions. Both the geographic location and the common historical background seem to work in Russia's favour over other regional power centres. The main targets of Russia's geopolitical ambitions are Georgia, Ukraine, Armenia, Belarus, Moldova, and Kazakhstan as sort of 'low-hanging fruits' due to their distance from Western associations. Yet this could also apply to the Baltic countries as, from Russia's perspective, the application of the neo-imperial model clearly depends upon particular conditions being in Russia's favour. In addition, Russia has used the economic lever, especially trade conditions, to punish Estonia and other Baltic states in the past for perceived incorrect political choices (Veebel *et al,* 2020). Therefore, Russia's past moves, its aggressive behaviour, and its neo-imperial ambitions in the international arena have definitely decreased the motivation of Estonian politicians and entrepreneurs to deepen economic ties with Russia in the nearest future, making them instead more cautious about Russia in general.

The prospects for the recovery of trade flows between the neighbours also presents Estonia (and other EU member states) with a moral problem. In other words, there is the question of whether it would be ethical to sacrifice the security of one's country to cooperate with a state that is constantly threatening you and does not share the same values as you. In this light, and from the Estonian perspective, it is somewhat astonishing to see that despite violent conflicts, mutual sanctions, and constant accusations, trade relations between Russia and Ukraine are intensifying again after the annexation of Crimea (see Figure 2), and that in 2018, Russia remains the main trading partner for Ukraine (TASS, 2019).[1] Be

[1] Only recently, in the first quarter of 2019, has Poland became the number one export market for Ukrainian goods (Business Ukraine, 2019).

that as it may for Ukraine, it is difficult for Estonia to accept that one can simultaneously declare unwavering support for territorial integrity and the independence of sovereign countries in the international arena, and to request cooperation in other issues with a state that has illegally annexed Crimea (for further discussion, see Veebel and Markus, 2018).

FIGURE 2: Ukraine's imports and exports with Russia in 2010–2018 (in billions USD).

Source: Trading Economics, 2019.

6. WIDENING THE SCOPE OF THE DISCUSSION: STRUCTURAL TRANSITION FROM LIBERAL TO POST-LIBERAL INTERNATIONAL ORDER

The three Baltic countries, along with the entire Baltic Sea region, are experiencing a series of deep transformations which, in the current academic literature, are associated with the drastic deterioration of Europe's relations with Russia in the aftermath of the annexation of the Crimea and the war in Donbas. Yet in a broader sense these changes are part and parcel of a structural transition from liberal to post-liberal international order, a non-linear process that differently affects regions that have been supported by the direct sponsorship of the EU. The ongoing transfiguration of the liberal order lacks clear logic and encompasses a number of politically consequential developments that directly affect the Baltic countries. Russia is clearly interested in exploiting this weakness, showing that the West is weak and helpless, and that '*the current crisis of liberalism will definitively bury the unipolar Western system of hegemony*', to quote the Russian media. Furthermore, Russia's media argues that populism and regional protectionism could serve as the basis for a new, multipolar world order (see Savin, 2018).

Next to the fundamental changes in the international order, the bulk of current dynamics seems to be grounded in the *de facto* fragmentation of the Baltic Sea region into three largely disconnected spheres. First of these is the EU-promoted normative space of good and liberal governance. Second is the Russo-German bilateral 'energy regionalism', which is exemplified by the Nord Stream project. Third is the resurgent domain of the regional security complex with its dominant logic of military deterrence. Besides this, it is becoming increasingly clear that Poland is interested in promoting the Intermarium project and participating in the Three Seas Initiative, but not so much in political investment in terms of region-building for the Baltic Sea area. Developments in adjacent Northern Europe range from the re-actualisation of Nato membership discourses in Finland and Sweden, coupled with the drastic deterioration of Russo-Norwegian relations, to the recent initiative of the Barents Council which is aimed at creating a visa-free Barents area regime in spite of the extant Schengen regulations. These new circumstances, trends,

and processes create a new, much more multifarious and less predictable (geo)political environment for the Baltic countries. The complexity of those political transmutations that have briefly been described above is a challenge for each of them. The gap between the Baltic countries and Russia has widened during the last five years. After 2014, the security aspects should definitely not be analysed solely in terms of strategic and geopolitical interaction between the West and Russia. The Baltic countries have been among the most concerned in the EU regarding Russia's potential actions. The fears and worries that have been experienced and expressed by Baltic societies and politicians have been heard by their Western partners, including European Union institutions. This is clearly reflected in plans and undertakings to deal with disinformation, and with military and hybrid threats against the EU, including the build-up of PESCO, the European Defence Fund, and provisioned expenditure from the MIFF in 2021–2027. These developments demonstrate a clear case of Europeanisation from the bottom-up (or 'uploading'), in which Estonian, Latvian, and Lithuanian concerns (in the form of principles and values) in terms of defending the Baltic countries have had an effect when it comes to changing perspective and attitude towards security issues at the supranational EU level. However, the question still remains whether this is enough to deter Russia in creating instability in the Baltic Sea region and in putting pressure on the Baltic countries.

CONCLUSIONS

The article has aimed at a discussion of the prospect for economic relations between Estonia and Russia against the background of reciprocal strategic narratives on both sides. Estonia's strategic narrative of Russia today is strongly influenced by the country's historical experience, the differentiation between Estonians and Russians, and the security threats that stem from Russia. Based on the national strategic narrative, Russia clearly remains an adversary for Estonia. Other potential visions, such as 'Estonia as a bridge between East and West' or 'Estonia as a positive influencer', are today out of the picture. In turn, Russia's national strategic narrative also seems to speak against improving relations with Estonia. Russia's current domestic image is based on the vision that 'Russophobic' and 'hysterical' enemies are surrounding it. The country also prefers to use the ideology of 'selective multipolarity', particularly in its relations with the EU, which allows the country to feel itself as being as important as Western countries as far as the security environment in Europe is concerned. Next to that, Russia constantly argues that Estonia does not respect the rights of its Russian minorities, and so on.

Therefore, it can clearly be seen that there are fundamental differences in national strategic narratives between Estonia and Russia, particularly in the way in which both countries interpret their common historical past, recognise the validity of international law, and understand their roles in the international arena. In this light, the blooming of trade relations between Estonia and Russia in the nearest future is rather unlikely, because there is simply no common ground upon which to develop mutual economic contacts. Furthermore, both the economic sanctions between Russia and the Western countries which are set limit to further economic cooperation between Estonia and Russia, as well as Russia's aggressive behaviour and neo-imperial ambitions in the international arena, serve to decrease the motivation of Estonian politicians and entrepreneurs when it comes to deepening trade relations with Russia in the nearest future. Theoretically, the recovery of trade relations between Estonia and Russia is possible under certain circumstances. Still, in practice the strengthening of economic cooperation between these neighbours is unlikely due to various security aspects.

However, as far as the conflicting strategic narratives of both countries are concerned, Estonia has made the first effort to rewrite Estonia's current strategic narrative for Russia as an enemy. As it contemplates with the wish to replace it with the new one, of Estonia as a bridge between East and West, there are some loose ends that could potentially be tied up, assuming that Estonia is interested in developing economic contacts with Russia. Firstly, in the future Estonia should keep a careful eye on all EU initiatives that are targeted towards Russia, particularly towards the upgrading of the EU-Russia cooperation programme and calls for a 'new partnership' with Russia that have been suggested by some EU member states within the framework of the European strategic autonomy initiative. Secondly, it would be reasonable for Estonia to do everything within its power to reconcile any differences between Estonians and Russian-speaking minorities in Estonia. This would leave Russia without its main argument in justifying its aggressive ambitions in neighbouring countries which, as far as Russia is concerned, are fully justified due to the 'unacceptable conditions' for Russian-speaking minorities in those countries and which entail Russia's 'responsibility' for protecting Russian-speaking populations in those countries. Last but not least, although any radical regime shift in Russia is rather unlikely due to the absence of a strong and united opposition and a lack of political alternatives in Russia, Western countries, including Estonia, should also be prepared for such potential developments. Consistent unrest in Russia over the past few years is a clear sign that not all people in Russia welcome the direction in which Vladimir Putin's Russia is currently heading.

Contacts:

Viljar Veebel
Baltic Defence College,
Department of Strategic Studies
E-mail: viljar.veebel@ut.ee

Raul Markus
Tallinn University of Technology,
School of Engineering, Department of
Mechanical and Industrial Engineering
E-mail: raul@optium.ee.

Liia Vihmand
Tartu University,
College of Foreign Languages
and Cultures
E-mail: liia.vihmand@ut.ee.

REFERENCES AND SOURCES

Andžāns, M.; Veebel, V. (2017). Deterrence Dilemma in Latvia and Estonia: Finding the Balance between External Military Solidarity and Territorial Defence. Journal on Baltic Security, Vol. 3.

Business Ukraine (2019). Ukraine turns West: Poland replaces Russia as the number one Ukrainian export market. Published on 1 May 2019. http://bunews.com.ua/economy/item/ukraine-turns-west-poland-replaces-russia-as-top-ukrainian-export-market

Cavegn, D. (2017). Opinion digest: The beginning of the end for the Baltic states. ERR, published on 18 July 2017. https://news.err.ee/608070/opinion-digest-the-beginning-of-the-end-for-the-baltic-states

Cooper, B. (2018). Changes in Estonian Defense Policy Following Episodes of Russian Aggression. Inquiries Journal, 10(10). http://www.inquiriesjournal.com/a?id=1745

De Graaf, B.; Dimitriu, G.; Ringsmose, J. (2015). Strategic Narratives, Public Opinion, and War. Routledge: London and New York.

Doroško, T.; Nutt, M.; Pääbo, H.; Riim, T.; Sillaste, J.; Tiiman, A.; Tüür, K.; Vare, R. (2004). Eesti Venemaa-poliitika lähtealused (available only in Estonian). https://www.riigikogu.ee/wpcms/wp-content/uploads/2014/11/Eesti-Venemaa-poliitika-l.pdf

Ellyatt, H. (2016). Russia hits back at „anti-Russian' NATO „hysteria'. CNBC, publsihed on 8 July 2016. https://www.cnbc.com/2016/07/08/russia-hits-back-at-anti-russian-nato-hysteria.html

ERR (2019a). Blogiülevaade: president Kaljulaid kohtus Moskvas Vene riigipeaga. Published on 18 April 2019 (available only in Estonian). https://www.err.ee/931293/blogiulevaade-president-kaljulaid-kohtus-moskvas-vene-riigipeaga

ERR (2019b). Rahvas ootab Eesti-Vene tippkohtumiselt majandussuhete elavdamist. Published on 17 April 2019 (available only in Estonian). https://www.err.ee/930909/rahvas-ootab-eesti-vene-tippkohtumiselt-majandussuhete-elavdamist

ERR (2019c). President Kaljulaid proposes updating EU-Russia cooperation. Published on 18 April 2019. https://news.err.ee/931687/president-kaljulaid-proposes-updating-eu-russia-cooperation

ERR (2019d). Kaljurand: presidendi Moskvas-käigus oli palju ebamäärast. Published on 23 April 2019 (available only in Estonian). https://www.err.ee/932749/kaljurand-presidendi-moskvas-kaigus-oli-palju-ebamaarast

ERR (2017). Russian foreign minister: Baltic states' claims about Russian threat absurd. Published on 29 March 2017. https://news.err.ee/586920/russian-foreign-minister-baltic-states-claims-about-russian-threat-absurd

Fefilov, D. (2019). Kuidas kajastasid Kaljulaidi ja Putini kohtumist vene telekanalid? Äripäev (*Business Daily Estonia*), published on 19 April 2019 (available only in Estonian). https://www.aripaev.ee/uudised/2019/04/19/kuidas-kajastasid-kaljulaidi-ja-putini-kohtumist-vene-telekanalid

Financial Times (2016). Putin names NATO among threats in new Russian security strategy. https://www.ft.com/content/6e8e787e-b15f-11e5-b147-e5e5bba42e51

Joao, A. (2017). Russia's Sanctions Narrative in the Ukrainian Crisis: Implications for the West. Revista UNISCI.

Kramer, M. (2003). NATO, Baltic states and Russia: a Framework for Sustainable Enlargement. International Affairs, Vol. 78, No. 4.

Made, V. (2004). Eesti ja Venemaa suhted rahvusvahelises taustsüsteemis. Eesti Diplomaatide Kool (available only in Estonian). https://www.riigikogu.ee/wpcms/wp-content/uploads/2014/11/Eesti-ja-Venemaa-suhted-rahvusvahelises-tausts.pdf

Mauricas, Z. (2015a). The effect of Russian economic sanctions on Baltic States. Overview of the Nordea Bank AB. https://nexus.nordea.com/research/attachment/17231

McKew, M. K. (2018). They will die in Tallinn': Estonia grids for war with Russia. POLITICO, published on 11 June 2018. https://www.politico.eu/article/estonia-rusia-nato-defense-they-will-die-in-tallinn-estonia-grids-for-war/

Miskimmon, A., O'Loughlin, B., & Roselle, L. (2017). *Forging the world: Strategic narratives and international relations*. University of Michigan Press.

Morozov, V. (2004). Russia in the Baltic Sea Region: Desecuritization or Deregionalization? Cooperation and Conflict, Vol. 39, Issue 3, pp. 317-331. https://journals.sagepub.com/doi/10.1177/0010836704045207

National Security Concept (2017). Published by Riigikantselei. https://www.riigikantselei.ee/sites/default/files/content-editors/Failid/national_security_concept_2017.pdf

Oja, K. (2015). No milk for the Bear, the impact to the Baltic states of Russia's counter sanctions. Baltic Journal of Economics, Vol. 15(1), pp. 38-49.

Osborn, A., Zverev, A. (2018). European politicians call for new sanctions on Russia over Ukraine. Reuters, published on 27 November 2018. https://www.reuters.com/article/us-ukraine-crisis-russia-germany/european-politicians-call-for-new-sanctions-on-russia-over-ukraine-idUSKCN1NW0WW

Pealinn (2018). Mikser seab Eesti-Vene suhted sõltuvusse Venemaa käitumisest. Published on 28 December 2018 (available only in Estonian). http://www.pealinn.ee/tagid/koik/mikser-seab-eesti-vene-suhted-soltuvusse-venemaa-kaitumisest-n234058

Ploom, Illimar; Sliwa, Zdzislaw; Veebel, Viljar (2020). The NATO 'Defender 2020' exercise in the Baltic States: Will measured escalation lead to credible deterrence or provoke an escalation? Comparative Strategy, 39 (4), 368–384. 10.1080/01495933.2020.1772626.

Piirsalu, J. (2018). Moskva Balti-ekspert: isegi „positiivne käitumine' ei anna Eestile sama rolli mis Soomele. RKK/ICDS publications „Diplomaatia', published on 16 March 2018 (available only in Estonian). https://diplomaatia.ee/moskva-balti-ekspert-isegi-positiivne-kaitumine-ei-anna-eestile-sama-rolli-mis-soomele/

Pääbo, H. (2011). Kollektiivse mälu konfliktid endise Vene impeeriumi aladel. ABVKeskuse Mõttepaber, No 2011/3 (available only in Estonian). http://www.ut.ee/ABVKeskus/sisu/paberid/2011/pdf/Malukonfliktid_Paabo.pdf

Ratso, S. (2015). EU-Russia Trade Relations in Light of Sanctions and Russia´s Import Measures. Diplomaatia, March 2015. Retrieved from http://www.diplomaatia.ee/en/article/eu-russian-trade-relations-in-light-of-sanctions-and-russias-import-measures/

Roth, M. (2009). Bilateral Disputes between EU Member States and Russia. CEPS Working Document, No. 319/August 2009.

Russkiy Mir (2019). Lavrov: Joint schools in Estonia infringe Russian children's rights. Published on 16 January 2019. https://russkiymir.ru/en/news/251255/

Savin, L. (2018). The death of the liberal world order. Geopolitics.ru, published on 29 March 2018. https://www.geopolitica.ru/en/article/death-liberal-world-order

Schatz, E. (2007). Framing Strategies and Non-Conflict in Multi-Ethnic Kazakhstan. Nationalism and Ethnic Politics, Vol. 6, No. 2, pp. 71-94.

Sirp (2015). Mida teha venelastega? Published on 9 January 2015 (available only in Estonian). http://www.sirp.ee/s1-artiklid/c9-sotsiaalia/mida-teha-venelastega/

Statistics Estonia (2019). Database: VK09: KAUPADE EKSPORT JA IMPORT RIIGI JÄRGI (KUUD) (available only in Estonian). http://pub.stat.ee/px-web.2001/ Dialog/varval.asp?ma=VK09&ti=KAUPADE+EKSPORT+JA+IMPORT +RIIGI+J%C4RGI+%28KUUD%29&path=../Database/Majandus/25Valiskaubandus/ 03Valiskaubandus_alates_2004/&lang=2

Stoicescu, K. (2015). Vene oht Läänemere piirkonna julgeolekule. RKK/ICDS publications „Taustapaberid' (available only in Estonian). https://icds.

ee/wp-content/uploads/2015/Kalev_Stoicescu_-_Vene_oht_Laanemere_piirkonna_julgeolekule.pdf

Tamberg, A. (2016). Eesti kuvand Venemaa online-meedias 2015. aastal julgeoleku seisukohalt. Sisekaitseakadeemia (available only in Estonian). https://digiriiul.sisekaitse.ee/bitstream/handle/123456789/39/2016_Tamberg%20.pdf?sequence=1&isAllowed=y

TASS (2019). Russia remains Ukraine's key trade partner in 2018, says statistics service. Published on 19 February 2019. https://tass.com/economy/1045433

The Embassy of the Russian Federation to the United Kingdom of Great Britain and Northern Ireland (2018). Foreign Minister Sergey Lavrov's remarks at Bolshaya Igra (Great Game) talk show on Channel One, Moscow, September 4, 2018. https://rusemb.org.uk/article/524

Trading Economics (2019). Ukraine - Economic Indicators. https://tradingeconomics.com/ukraine/indicators

Veebel, V. (2017). Russia's Neo-Imperial dependence model: Experiences of former Soviet republics. Romanian Journal of Political Science, Vol. 1.

Veebel, Viljar (2018). NATO options and dilemmas for deterring Russia in the Baltic States. Defence Studies, 18 (2), 1–23.

Veebel, Viljar (2019). Why it would be strategically rational for Russia to escalate in Kaliningrad and the Suwalki corridor. Comparative Strategy, 38 (3), 182–197.

Veebel, V., Markus, R. (2016). At the Dawn of a New Era of Sanctions: Russian-Ukrainian Crisis and Sanctions. Orbis, 60 (1), 128–139.

Veebel, V.; Markus, R. (2018). The bust, the boom and the sanctions in trade relations with Russia. Journal of International Studies, 11(1), pp. 9-20.

Veebel, V.; Markus, R.; Ploom, I. (2019). EU-financed peripheral large-scale infrastructure projects and white elephant syndrome: example of Rail Baltica. Acta Oeconomica, Vol. 69 (1), pp. 17–39.

Veebel, V; Vihmand, L.; Ploom, I.; Markus, R. (2020). Western Misperception when Deterring Russia: Cultural and Linguistic Factors. Journal of Politics and Law, 13 (3), 151–159.10.5539/jpl.v13n3p151.

Ventsel, A.; Hansson, S.; Madisson, M.-L. and Sazonov, V. (2019) *Discourse of fear in strategic narratives: The case of Russia's Zapad war games*, 'Media, War & Conflict', pp. 1–19

Välisluureamet (2019). International Security and Estonia (2019). https://www.valisluureamet.ee/pdf/raport-2019-ENG-web.pdf

USING MILITARY CONCEPTS IN CIVIL ADMINISTRATIVE STRUCTURES: THE ESTONIAN CASE

Diana Marnot, MSc
Estonian Academy of Security Sciences
Junior Research Fellow

Keywords: strategic communications, information operations, psychological operations, psychological defence

ABSTRACT

Estonian governmental authorities have imported terms like strategic communication, information operations, psychological operations, and psychological defence from NATO's military concepts into civil structures. This paper shows how questionable the use of the above terms in public administration vocabulary can be: e.g. 'information operations' and 'psychological operations' are, in essence, military tools used against adversaries. The paper aims to give a snapshot of the conceptual overviews of the terms 'strategic communications', 'information operations' 'psychological operations', and 'psychological defence'. It will show the importance of using precise terms by state administrative bodies. To achieve this, the author provides historical background for the borrowed terminology. Official Estonian, NATO and EU documents are also analysed to show the use and connotations of these terms. These steps provide the framework for the final discussion. The discussion shows how seemingly innocent terms can give very vast options for the government to use in peacetime with their citizens and friendly nations.

INTRODUCTION

Strategic communication, information operations, psychological operations, and psychological defence. What is the difference between these concepts and if, then where do they overlap? In the Estonian context, most of these concepts have been used by three governmental authorities: The Government Office of Estonia, the Headquarters of the Estonian Defence Forces, and the Estonian Ministry of Defence. All three authorities have departments or sections of strategic communication (SC). It would not make a difference if the understanding of SC were derived from the industry. However, the concepts above (except for psychological defence) are imported from NATO's military concepts into civil structures and understood in similar terms. That is the reason why Estonian governmental authorities associate SC with the terms 'information operations' (IO) and 'psychological operations' (PSYOPS). Why is this problematic? The terms IO and PSYOPS could be considered as great communication toolboxes when confronted with adversaries. So, in theory, Estonian governmental authorities have provided themselves with the option of using military communication strategies in a peace-time context.

The first Estonian governmental authority to rename their communication bureau into a SC department was the Headquarters of the Estonian Defence Forces (2013), followed by the Estonian Ministry of Defence (2014), and finally, in 2016, the Government Office of Estonia. It is also important to mention that the Government Office's communication unit was previously known to conduct 'psychological defence' (PsycDef), which was later regarded to be just one side of SC. So, it seems that the Government Office followed the steps of the HQ of the Defence Forces and Ministry of the Defence. The following question may thus be posed: on which grounds did the Estonian governmental authorities adopt the concept of 'strategic communications'? The aim of this article is to give a snapshot of the conceptual overviews of the terms 'strategic communications', 'information operations' 'psychological operations', and 'psychological defence'. A short overview is presented of how these concepts are employed in the United States of America and the European Union. The overview provides context for understanding the use of the conceptions in question by Estonian governmental authorities and the problems this

can lead to. The article is thus based on three research questions: What are the main differences between SC, IO, and PSYOPS? What is the connection between SC and IO for Estonian governmental authorities? Where is the overlap in concepts of SC and psychological defence?

1. METHOD

An inductive thematic analysis method was used in this article. As there was no previous study to base this one on, the codes with their interpretations were derived from the original texts (Vaismorardi, et al., 2013; Hsieh & Shannon, 2005). The data was compiled from academic articles and 'grey' literature, which included primarily governmental documents and military manuals. The only search terms used were 'strategic communication' and 'strategic communications'. As the intention of this study was to find the overlap with the notion of PsycDef, this helped minimise the number of results by discarding the term SC as it is used in the industry. As one of the research questions was also related to the connection of SC with IO and PSYOPS the search results falling under the sample criteria were related to the military and defence circles. Therefore, the sample was purposive, with the aim of interpretive explanation. It was chosen because the results of the conceptual definitions did not change after saturation of theoretical concepts were achieved (Thomas & Harden, 2008, p. 3; Doyle, 2003, p. 326).

At first, academic articles were searched using EBSCO Discovery and Sage Journals Online databases, but this search method exhausted itself fast. From the perspective of conceptual definition, the articles there, related to security and defence issues, were not useful for this study, as they lacked definitions of concepts. 'Grey' literature (governmental documents; army manuals; thematic books) was taken up next where more conceptual definitions were found. For this study, only the meanings of SC were collected and analysed.

The search was conducted between June 2017 and January 2018 and preliminary results written up between periods of data analysis. Overall, the concept SC was studied in 39 different sources. Data analysis and data collection were done simultaneously until the saturation of theoretical concepts was met. Quickly, it became clear that the term, although seemingly used in similar contexts, almost always contained some varieties, leaving no clear and unanimous definition. The QSR Nvivo10 software was used for data analysis. After the data had been transferred to the program it was all coded line-by-line to determine the interpretations of the concepts.

2. CONCEPTUAL UNDERSTANDING OF 'STRATEGIC COMMUNICATIONS', 'PSYCHOLOGICAL OPERATIONS', AND 'INFORMATION OPERATIONS' IN THE UNITED STATES OF AMERICA AND THE EUROPEAN UNION

The most conclusive article on SC divides the term across disciplines as follows (Hallahan, et al., 2007):

- Management communication that facilitates 'the orderly operations of the organisation';
- Marketing communication, aiming to 'promote sales of products and services';
- Technical communication, training employees and customers in using end-products;
- Public relations, to maintain 'mutually beneficial relationships with key constituencies';
- Informational/social marketing campaigns, aiming to better the community;
- Political communications, with the aim 'of building political consensus or consent on important issues involving the exercise of political power and the allocation of resources in society.' At the international level, this includes communications in support of public diplomacy and military stabilisation.

In the context of this article, the SC used in the Estonian governmental system can be considered to be political communication. In the political, more precisely in the military context, one of the most conclusive definitions of SC is one proposed by the RAND analyst Christopher Paul (2011, p. 3):

'/---/ coordinated actions, messages, images, and other forms of signalling or engagement intended to inform, influence, or persuade selected audiences in support of national objectives.'

However, things are not that simple. Defining SC is considered to be a problem because it is hard to delimit what it is and what it is not. There is a misbelief between actors, and '/---/ incorrect assumptions of shared understanding, and activities being labelled as part of strategic communication that many might think should be excluded' (Paul, 2011, p. 2). For example, should SC include only messaging, or is it more relevant to counter adversary propaganda (Paul, 2011, p. 12)? One of the sources of misunderstandings could be considered to be the US military's usage of IO and PSYOPS as parts of SC (Stavridis, 2007, p. 5).

Nevertheless, what does IO and PSYOPS in the US's military terminology exactly mean?

Information operations — 'The integrated employment, during military operations, of information-related capabilities in concert with other lines of operation to influence, disrupt, corrupt, or usurp the decision-making of adversaries and potential adversaries while protecting our own.' (DoD, 2017, p. 111; Joint Chiefs of Staff, 2014, p. GL-3).

Psychological operations – 'Psychological operations (PSYOPS) are planned operations to convey selected information and indicators to foreign audiences to influence the emotions, motives, objective reasoning, and ultimately the behaviour of foreign governments, organizations, groups, and individuals. PSYOPS are a vital part of the broad range of US diplomatic, informational, military, and economic activities. PSYOPS characteristically are delivered as information for effect, used during peacetime and conflict, to inform and influence.' (Joint Chiefs of Staff, 2003, p. ix)

Behavioural change has been seen as the root of a PSYOPS mission (Department of the Army Headquarters, 2005, p. 2). PSYOPS also cover 'counterpropaganda operations': 'Those psychological operations activities that identify adversary propaganda, contribute to situational awareness, and serve to expose adversary attempts to influence friendly populations and military forces' (Joint Chiefs of Staff, 2003, p. GL-5).

In the context of this article, some elements of PSYOPs need to be emphasised. The roles of PSYOPs are, as described by the Department of the Army Headquarters (2005, p. 3):

- Influence foreign populations by expressing information subjectively to influence attitudes and behaviour. Also, to obtain compliance, noninterference, or other desired behavioural changes.

- Provide public information to foreign populations to support humanitarian activities, restore or reinforce legitimacy, ease suffering, and maintain or restore civil order.

- Serve as the supported commander's voice to foreign populations to convey intent and establish credibility.

- Counter enemy propaganda, misinformation, disinformation, and opposing information to portray friendly intent and actions correctly and positively for foreign target audience's, thus denying others the ability to polarize public opinion and political will against the United States and its allies.

The idea of using military PSYOPs at the level of national communication is not new. Already in 1983, it was declared that the US needs PSYOPs to be part of a national security strategy as a peacetime weapon, to be employed worldwide for furthering American objectives (Paddock, 1983 pp. 1–2). The distinction between PSYOPS as a tool for managing neutral or helpful information versus PSYOPS as a weapon became obscure in military thought already in the 1990s (Badsey, 2015, p. 195).

The interpretation of the military concept of PSYOPS as a part of regular national political strategy regained its popularity in public papers after 9/11 and the war in Afghanistan. This time, however, there discussions revolved around SC. A report by the Federal Advisory Committee, the Defence Science Board (2004, p. 11) recommends that the United States DoD should manage 'policies, diplomacy, military operations, and strategic communication' as a whole. A report from the Congressional Research Service about the DoD describes SC as being supported by IO and primarily through PSYOPS. When DoD uses SC, it means

interacting 'with and influencing foreign publics, military adversaries, partner and non-partner governments, other US government agencies, and the American people' (Nakamura & Weed, 2009, p. 28). The report by the Defense Science Board (2004, p. 11) described SC as helping shape context and building relationships that 'enhance the achievement of political, economic, and military objectives'. It is also useful in mobilising 'publics in support of major policy initiatives – and to support objectives before, during, and after a conflict'. The last sentence is very similar to the statement in Colonel Paddock's (1983, p. 1) description of the use of PSYOPS: '/---/ the planned use of communication to influence attitudes or behavior should, if properly used, precede, accompany, and follow all applications of force'. Today's US military understanding of SC seems to be derived from three decade-old views of PSYOPS. Peacetime military action furthering civil goals in the US is thus not a novel strategy.

Similar distribution to the military's understanding has also been proposed by Professor Philip M. Taylor (2008, p. 14) who states that SC has four pillars: 'information operations, psychological operations, public diplomacy, and public affairs'. Some people do not even make the difference between SC and IO, as long as the objectives are reached and the information environment shaped as intended (Murphy, 2008, p. 3).

SC also has its place in the European Union. The increased propaganda and disinformation campaigns regarding the Ukrainian conflict, as well as the Daesh recruitment efforts have urged the European Union to take a stance on SC (Pawlak, 2016, p. 2). For this, the EU has set up an administrative body, the EastStratCom Task Force, and created an EU Action Plan (European Council, 2015, p. 1) with the following objectives:

- Effective communication and promotion of EU policies and values towards the Eastern neighbourhood.

- Strengthening of the overall media environment, including support for independent media.

- Increased public awareness of disinformation activities by external actors, and improved EU capacity to anticipate and respond to such activities.

The European Union does not declare that it is using IO or PSYOPS in its SC endeavours. However, the third objective, countering disinformation via various awareness-raising methods, suggests activities overlapping with the military term 'counterpropaganda operations', which is again similar to concept of PsycDef that has been used in Estonia.

NATO has its own SC unit which in its military context has its place and will not be elaborated more in this paper. However, it is essential to point out that in 2014, a NATO accredited Centre of Excellence on strategic communication (NATO StratCom COE) was founded. Its main focus areas include countering hostile propaganda, and raising awareness of mis- and disinformation (NATO StratCom COE, 2017). In 2015, the Centre published their first academic journal, *Defence Strategic Communication* (NATO StratCom COE, 2015). The term 'defence strategic communication' is the closest to the idea of SC being similar to 'counterpropaganda operations' and PsycDef. The word 'defence' seems to be used to inform the readers that there are indeed adversaries. It narrows down the objectives of SC, leaving only minimal possibilities for interpreting the concept. The interpretation that NATO has adopted via the abovementioned COE also solves the question of feedback posed by Cunningham (2010, p. 112). Namely, Cunningham states that when the goal of SC 'is to change perceptions, opinions, and ultimately behaviour', it is important to get some feedback for the evaluation of success. If SC is defined as broadly as it is in the US and EU, success is indeed difficult to measure. However, if the term is narrowed down, as it is with the prefix 'defence', it helps establish clear goals and means for the evaluation of the process.

3. PSYCHOLOGICAL DEFENCE IN ESTONIA

The concept of PsycDef was used or the first time in a public document in 2001 (Riigi Teataja, 2001). It was listed alongside 'civil defence', 'economic defence', 'civil readiness', and 'military defence' – all of which formed the concept of 'total defence'. According to this document, PsycDef was the responsibility of the Estonian Ministry of Education, which intended to 'shape the mentality of an independent democratic citizenry, furthering and maintaining the defence will of the citizenry during the time of crisis or war'. The task of the Ministry of Education was to promote the advantages of democratic governance. The term is the same as and its content very similar to one used in Sweden in the 1950s – *psykologiskt försvar* (in English 'psychological Defence'). This form of defence was the task of civil authority which was responsible for helping the Swedish population to resist any misinformation or rumours. The fear was that the perceptions of civilians or decision-makers of specific questions could be altered by an unfriendly country (Konnander, 2015). The aim thus was to protect the everyday information environment. The need for something similar for Estonia emerged after the collapse of the Soviet Union.

The effects of the Cold War and the Soviet occupation of Estonia were still visible in the 1990s. Although Estonia had regained its independence in 1991, the values and advantages of a democratic country were not self-evident. Parts of society, mostly of non-Estonian origin, were not in favour of an independent Estonia. Russian military troops were not relocated from Estonia until 1994, and the new neighbouring country tried to influence the perceptions of the international community by painting the newly-formed democratic country as a down-and-out country, with no credibly perspective. The threat of anti-Estonian propaganda was thus ever-preset. The developments of the 1990s lead to the formation of a defence strategy built around the concept of 'total defence', which included 'psychological defence'. Nonetheless, Estonia continued to develop and evolve as a peaceful democratic country, which resulted in joining the European Union and NATO in 2004.

At the same period, in 2000, Vladimir Putin became the president of the Russian Federation. During his presidency, he started to pull Russia

out of the chaos of the 1990s, to regain its imperial glory. This process culminated in 2005, with the celebration of the 60 year anniversary of the victory of the Soviet Union in WWII. These celebrations also resulted in the glorification of the Soviet Union, which directly led to the Bronze Night in Estonia in 2007: a massive riot which for some time-period polarized the society between Russians and Estonians (for more, see: Davydova, 2008; Hackmann & Lehti, 2010; Lehti, et al., 2008; Pääbo, 2008; Selg, 2013; Wertsch, 2008). One of the reasons for these events were the two information rooms people were living in which had a polarising effect on the Estonian society. Russian propaganda continued to besiege Estonia until the Russo-Georgian war, after which Russia's attention shifted toward a new enemy.

It has been stated (Ministry of Defence, 2013) that because Estonia is an open society, it also has an open information environment, which makes it an easy target for hostile influence activities. Preserving and developing national defence is thus the responsibility of all agencies and governmental authorities with national defence functions (Ministry of Defence, 2014). The aim was to preserve and defend the society in peacetime, hopefully avoiding any provoked conflicts that could lead to an actual war. The propaganda campaigns and cyber-attacks against Estonia in 2007 showed that the information environment also needs to be included in the state-defence programme. This culminated with the adotion of a new security policy, 'National Security Concept of Estonia' (Riigikogu, 2010). The policy states that 'A broad security concept entails the involvement of all sectors of the society, as well as an integrated approach, where the foreign policy, defence policy and internal security policy, as well as cohesion and resilience of the society, are employed to achieve the security policy goals for the country as a whole' (Riigikogu, 2010, p. 3). The policy is directed at preventing and, should the need arise, repelling military threats. In this document, PsycDef is defined as follows (Riigikogu, 2010, p. 20):

'Psychological defence is the development, preservation, and protection of common values associated with social cohesion and the sense of security. The aim of psychological defence is to safeguard the security of the state and society, to enhance the sense of security, to avert crises, and to increase trust amongst society and towards the actions taken by the state. Psychological defence facilitates the strengthening of the nation's

self-confidence and the will to defend Estonia. Psychological defence and the recognition of constitutional values strengthen the resilience to avert anti-Estonian subversive activity. Psychological defence is developed in co-operation with all members of the civil society.'

The next document to reaffirm the idea of a comprehensive national defence and PsycDef was the National Defence Strategy (Estonian Ministry of Defence, 2011). According to this document (2011, p. 3): '/…/ the most serious potential threats to Estonia derive from hybrid and combined challenges and a combination of internal and external developments. Therefore, the national defence can no longer be limited to military defence alone. Only a comprehensive approach to defence can guarantee a country's security.' Which in itself concluded again that '/…/ all major Estonian state authorities shall participate in national defence, thus combining military forces with non-military capabilities.' (Estonian Ministry of Defence, 2011, p. 3) This document went into more detail in defining PsychDef. Its aim '/…/ is to prevent panic, the spread of hostile influences and misinformation, thereby ensuring continued popular support to the state and its national defence efforts.' (Estonian Ministry of Defence, 2011, p. 3)

So there is a visible parallel with the terms PsycDef and one of the tasks of PSYOPS, which was to counter enemy propaganda, misinformation, disinformation, and opposing information to portray friendly intent and actions correctly and positively for foreign TAs, thus denying others the ability to polarise public opinion and political will against the United States and its allies.

4. STRATEGIC COMMUNICATION TIMELINE IN ESTONIA

There are three governmental authorities in Estonia using the term SC: the Estonian Government Office, Estonian Ministry of Defence, and the Headquarters of the Estonian Defence Forces. The Headquarters of the Estonian Defence Forces adopted the concept in 2013. The department formerly known as the Notification Department was renamed into the Department of SC. The reason given was that notification was just one part of the department's tasks. Aside from announcements, communication also entails IO, PSYOPS, and civic-military co-operation (CIMIC) – and they all come together under the term 'strategic communication' (Mölder, 2013, p. 3).

Soon after, in 2014, the term 'SC' was also put to use in the Estonian MoD. The ministry's statutes (Riigi Teataja, 2014) were changed, renaming the 'public relations' department to 'strategic communications'. The department participates in the management and coordination of national and NATO SC. It manages and coordinates the planning and implementation of communication activities between ministries and the government, including informing the public about national defence and defence policy issues. It also controls and coordinates communication between local governments and the allocation of grants to social organisations from the budget of the respective sphere of government.

In 2015, the Estonian Government Office created the position of a Psychological Defence Advisor. This position was created under the Government Communication Unit. The primary obligations for this position were the organisation of PsychDef development, coordinating government communication on security and state defence issues, and also analysing the security aspects of the information environment (Jõesaar, 2014). A year later, the advisor at the time claimed in his article (Raag, 2016) that the term PsychDef as a governmental ability to defend the communication environment has not been successful. He stated that many activities known to PsychDef were known in the West as SC. As the position holder, it was his initiative to rename the advisory position in the Government Office to a 'Strategic Communication Advisor'.

Finally, the last relevant document, the National Defence Development Plan 2017–2026 (Riigikantselei, 2017), defines various courses of actions for national defence. Among other things, SC is defined as one of the priorities which also include PsycDef. The document presents these two activities as separate notions, which is yet again a new development. It is more similar to the scheme where IO incorporates PSYOPS. According to this document, the goal of SC is to provide support to Estonian security policy, maintain public awareness of security situations, and avoid panic among the population. It also aims to neutralise hostile actions and uncover false information, preventing its spread. SC involves planning and centralising all state activities into one communicative whole and mediating it to society.

In summary, the concept used in Estonian governmental authorities has evolved from plain public relations and communications into SC. The Government Office created the position of a PsycDef advisor and soon transformed this into an SC position. Both the MoD and the Headquarters of the Defence Forces adopted their concepts of SC from the the US. As a result, they probably also view themselves as using IO and PSYOPS as parts of their communication activities. The Government Office replaced with SC because it overlaps in some parts with PSYOPS, which is defined under IO, providing a justification adopting the US military definition of SC. However, it is interesting to consider why the Estonian Government Office is involving itself in SC, which comes with the same toolbox that militaries use against adversaries. The question has been posed before whether governmental authorities, especially the Government Office, as public institutions should use SC as a means for public diplomacy. Dyke & Verčič (2009, p. 823) point out that the '/---/ credibility and efficacy of public relations and public diplomacy might be put under question when mixing SC and military IO.'

5. DISCUSSION

So what does it mean when a government declares itself to be using SC which can be confused with the military concept of SC? Thinking about this for a moment, it might appear that when a government claims itself to be using SC which entails IO and PSYOPS, this could be a cause for concern. The DoD defines IO as '[t]he integrated employment, during military operations, of information-related capabilities in concert with other lines of operation to influence, disrupt, corrupt, or usurp the decision-making of adversaries and potential adversaries while protecting our own.' (DoD, 2017, p. 111) Whereas armed conflicts entail a clear adversary, the target audience of peacetime SC can include foreign audiences, partner and non-partner governments – almost anyone. IO in a military context has numerous instruments at its disposal, among which we may list, e.g. MILDEC (military deception) and EW (electronic warfare). These examples are chosen knowingly as drastic and dramatic. However, the aim here is to make you wonder: why should a civil governmental authority appoint itself these capabilities when interacting with friendly parties, such as its citizens and partner governments? The Estonian MoD and HQ of Estonian Defence Forces describe their SC as being part of informing the local public of various activities, as well as defending public interests. This, however, entails means only known to them and specifics also only known to them. So they are open concerning what they are doing, but not how they are doing it.

Another point also bears consideration. The role of PSYOPS is to provide public information to foreign populations for whatever reasons necessary. This inevitably leads to the question of the clash of authorities. If the Ministry of Defence or the Headquarters of the Defence Forces have given themselves the right to interact with foreign populations, then where does it leave the diplomatic services? It is just another example of confusions that might arise when concepts, such as SC or PSYOPS, are taken to represent some official tasks of a state administrative body.

The author of this text does not hold the position that, e.g. Estonian governmental authorities have the intentions of using their communication abilities similarly on the local population as they would do in wartime

with adversaries. Alternatively, use techniques that they hypothetically could. The idea is to point out that the terms discussed in this paper are meant to describe actions used as state instruments. One decision that could fall under this critique is the replacement of PsycDef with SC by the Government Office. The former has distinctively defencive aims and functions. Because SC is defined in other fields so broadly and diversely, it has become challenging to understand what is exactly meant by it - what actions does this activity entail? This leads to the possibility that with the usage of the concept of SC, some publicly not so agreeable communication methods and aims might be used. In essence, as a government tool, SC can mean whatever: all actions and intentions that a selected government undertakes could be labelled as SC. Therefore the term is confusing and foggy, which should not be appropriate when describing governmental activities. To put it simply, in the Estonian case, it is the combination of usual PR and PsycDef. However, the term PR leaves enough options to present the government activities in a variety of ways – also leaving room for propagandist aims, if need be. PsycDef again is a security issue that too could fall under the governing area of an acting government but perhaps not under everyday communication activity.

CONCLUSION

The question of Estonian MoD and HQ of the Defence Forces using PSYOPS and IO as everyday communication activities can be considered relevant for the military environment. The US and NATO have been a role model for these decisions. Therefore, there is nothing remarkable about the adaptation of these terms in the Estonian military spheres. Another question is to consider whether the Estonian Government Office is the right institution to copy the military's modus operandi. It leaves room for questioning whether the Government Office might overstep its power and jurisdiction.

Furthermore, one might also take into account the possibility that this is a kind of a mechanism for adaptation to the new security environment – to so-called hybrid threats. For this reason, the state institutions are creating some sort of a new system of hybrid defence, which accounts for the fact that information warfare is an ever-present threat to the society.

This article focused the definition of SC and similar concepts, such as PSYOPS, IO, and PsycDef. The concepts were compared and their meanings analysed. The outcome of this study is a good foundation for future research on similar topics.

Contact:

Diana Marnot
Estonian Academy of Security Sciences
E-mail: diana.marnot@sisekaitse.ee

REFERENCES AND SOURCES

Badsey, S., 2015. Bridging the Firewall? Information Operations. In: *Propaganda, Power and Persuasion.* London. New York: I.B. Tauris, pp. 188-206.

Cunningham, T., 2010. Strategic Communication in the New Media. *Joint Force Quarterly*, Issue 59.

Davydova, O., 2008. Bronze soldier goes transnational: mediascapes and the formation of identities in internet discussions. *Ethnopolitics,* 7(4), pp. 391-411.

Defense Science Board, 2004. *Report of the Defense Science Board Task Force on Strategic Communication,* Washington: Defense Science Board.

Department of Defence, 2001. Propaganda. In: *Joint Pub 1-02.* s.l.: s.n., p. 434.

Department of the Army Headquarters, 2005. *FM 3-05.30 Psychological Operations,* Washington: s.n.

DoD, 2017. Information operations. In: *DoD Dictionary of Military and Associated Terms.* s.l.: Department of Defense, p. 111.

Doyle, L. H., 2003. Synthesis through meta-ethnography: paradoxes, enhancements, and possibilities. *Qualitative Research,* 3(3), pp. 321-344.

Dyke, M. A. V. & Verčič, D., 2009. Public relations, public diplomacy, and strategic communication: an international model of conceptual convergence. In: K. Sriramesh & D. Verčič, eds. *The Global Public Relations Handbook: Theory, Research and Practice. Revised and Expanded Edition.* New York and London: Routledge.

Eder, G. M. K., 2007. Toward Strategic Communication. *Military Review*, July-August.

Estonian Ministry of Defence, 2011. *National Defence Strategy Estonia.* Available at: www.kaitseministeerium.ee/sites/default/files/elfinder/.../national_defence_strategy.pdf [Accessed: 01.03.2018].

European Council, 2015. *Action Plan on Strategic Communication,* s.l.: s.n.

Gerth, J., 2005. Military's Information War Is Vast and Often Secretive. *The New York Times*, 11 December.

Hackmann, J. & Lehti, M. eds., 2010. Introduction. In: *Contested and Shared Places of Memory: History and Politics in North Eastern Europe* . New York: Routledge, pp. 1-3.

Hallahan, K., Holtzhausen, D., Ruler, B. v. & Verčič, D., 2007. Defining Strategic Communication. *International Journal of Strategic Communication,* 1(1), pp. 3-35.

Huntemann, N. B. & Payne, M. T. eds., 2010. *Joystick Soldiers: The Politics of Play in Military.* s.l.: Taylor & Francis.

Joint Chiefs of Staff, 2003. *Joint Publication 3-53: Doctrine for Joint Psychological Operations.* s.l.: s.n.

Joint Chiefs of Staff, 2012. *Joint Publication 3-13.1 Electronic warfare.* s.l.: s.n.

Joint Chiefs of Staff, 2014. *Joint Publication 3-13. Information Operations.* Washington, DC: s.n.

Jõesaar, T., 2014. Ilmar Raag hakkab psühholoogilist kaitset arendama. *Eesti Päevaleht*, 31 12.

Konnander, F., 2015. *Psykologiskt försvar.* Available at: http://www.sakerhetspolitik.se/Forsvar/psykologiskt-forsvar/ [Accessed: 01 March 2018].

Lehti, M., Jutila, M. & Jokisipila, M., 2008. Never-ending Second World War: public performances of national dignity and the drama of the Bronze Soldier. *Journal of Baltic Studies,* 39(4), pp. 393-418.

Ministry of Defence, 2013. *National Defence Development Plan 2013-2022.* Available at: http://www.kaitseministeerium.ee/riigikaitse2022/riigikaitse-arengukava/index-en.html [Accessed 01 March 2018].

Ministry of Defence, 2014. *Defence planning.* [Online] Available at: http://www.kaitseministeerium.ee/en/objectives-activities/defence-planning [Accessed on 1 March 2018].

Murphy, D. M., 2008. *The Trouble with Strategic Communication(s),* s.l.: Center for Strategic Leadership, U.S. Army War College.

Mölder, A., 2013. *Seletuskiri kaitseministri määruse 'Kaitseväe Peastaabi põhimäärus' eelnõu juurde,* s.l.: s.n.

Nakamura, K. H. & Weed, M. C., 2009. *U.S. Public Diplomacy: Background and,* s.l.: CRS Report for Congress.

NATO StratCom COE, 2015. *Academic journal 'Defence Strategic Communications' Vol 1.* Available at: https://www.stratcomcoe.org/academic-journal-defence-strategic-communications-vol1 [Accessed: 01 March 2018].

NATO StratCom COE, 2017. *About us.* Available at: https://www.stratcomcoe.org/about-us [Accessed 01 March 2018].

Paddock, A. H., 1983. *Military Psychological Operations and US Strategy.* [Online] Available at: https://consortiumnews.com/wp-content/uploads/2017/02/MilitaryPSYOPSandUSstrategy-Paddock.pdf. [Accessed: 01 March 2018].

Paul, C., 2011. *Strategic Communication.* s.l.: Praeger.

Pawlak, P., 2016. *EU strategic communication with the,* s.l.: European Parliamentary Research Service.

Pääbo, H., 2008. War of memories: explaining 'memorials war' in Estonia.. *Baltic Security and Defence Review,* Volume 10, pp. 5-25.

Raag, I., 2016. *Ilmar Raag: psühholoogiline kaitse pole voodoo.* Available at: https://arvamus.postimees.ee/3570987/ilmar-raag-psuhholoogiline-kaitse-pole-voodoo [Accessed: 01 March 2018].

Riigi Teataja, 2001. *Eesti sõjalise kaitse strateegia kinnitamine.* Available at: https://www.riigiteataja.ee/akt/84779 [Accessed: 01 March 2018].

Riigi Teataja, 2014. *Vabariigi Valitsuse 27. aprilli 2004. a määruse nr 151 'Kaitseministeeriumi põhimäärus' muutmine.* Available at: https://www.riigiteataja.ee/akt/129122014004 [Accessed: 01 March 2018].

Riigikantselei, 2017. *RIIGIKAITSE ARENGUKAVA 2017–2026. Avalik osa.* Available at: https://riigikantselei.ee/sites/.../rkak_2017_2026_avalik_osa.pdf [Accessed: 25 February 2018].

Riigikogu, 2010. *National Security Concept of Estonia.* Available at: https://www.eda.europa.eu/.../estonia---national-security-concept-of-estonia-2010.pdf [Accessed: 01 March 2018].

Selg, P., 2013. A political-semiotic introduction to the Estonian 'bronze night' discourse. *Journal of Language and Politics,* 12(1), pp. 80-100.

Stavridis, J. G., 2007. Strategic Communication and National Security. *Joint Force Quarterly*, Issue 46.

Taylor, P. M., 2008. Public Diplomacy and Strategic. In: N. Snow & P. M. Taylor, eds. *Routledge Handbook of Public Diplomacy.* New York: Routledge, pp. 12-19.

Thomas, J. & Harden, A., 2008. Methods for the thematic synthesis of qualitative research in systematic reviews. *BMC Medical Research Methodology,* 8(45).

Vaismorardi, M., Turunen, H. & Bondas, T., 2013. Content analysis and thematic analysis: Implications for conducting a qualitative descriptive study. *Nursing & health sciences,* 15(3), pp. 398-405.

Wertsch, J. V., 2008. Collective memory and narrative templates. *Social Research: An International Quarterly,* 75(1), pp. 133-156.

UNDERSTANDING THE ESSENCE OF ETHNIC CONFLICT: A THEMATIC LITERATURE REVIEW

Helina Maasing, MA
Estonian Academy of Security Sciences
Research fellow
University of Tartu
PhD Student in Sociology

Keywords: ethnic conflict, literature review, ethnicity, grievances, mobilisation, group size

ABSTRACT

Although, there is a vast amount of literature on ethnic conflict produced in recent decades, there is no good systematic overview of the main arguments and hypothesis on the core themes around the triggers of ethnic conflict.This article asks about the main arguments and gaps in terms of ethnic conflict literature in three theme areas, all of which were identified in a keyword analysis involving the relationships between: 1) ethnicity; 2) the (perceived) grievances and opportunities between various groups; and 3) the role of a group's size in terms of groups being able to mobilise. This semi-systematic review is based on a total of 96 relevant scientific articles that have been published in English language journals since 1990. This review provides a roadmap for researchers in this field so that they can navigate through the extensive literature to be able to provide future research directions. The results of the review show that competing arguments prevail in the available literature. There is no commonly agreed explanation between scholars on what causes ethnic conflict. Rather, there are several competing and complementary hypotheses, each of which is debated by others. Different results are based on different forms of methodology and datasets. In order to further empirical knowledge and common understanding, I suggest that future research focuses on: 1) the role on the perceived grievances of groups that can serve to mobilise them, and therefore adopt meso-level and/or micro-level data variables to test known theories and hypothesis in relation to ethnic conflict; 2) to better the understanding of the role of ethnicity in the collective action; and 3) strengthen arguments about the relationship between polarisation and conflict.

1. INTRODUCTION

In recent decades, instead of the traditional interstate military conflict, we have seen the emergence of increasing amounts of sub-state identity-based violence (such as in Syria, Iraq, Yemen, Rwanda, the Balkan states that formerly made up Yugoslavia, and Nagorno-Karabakh). This has also spiked the interest of scholars and policy analysts when it comes to better understanding the potential for an outbreak of ethnic strife and the evolution of power relations in the region. Robert Malley from the International Crisis Group points out that local conflicts serve as mirrors for global trends: the process governing how conflicts start, unfold, and are resolved reflect shifts in the relations between the great powers, the intensity of their competition, and the breadth of the ambitions of regional players. In addition, to be able to ensure cohesive communities and to develop preventive mechanisms, it is important to understand the origins and drivers of conflict between different ethnic groups.

An ethnic conflict is a confrontation between at least two contending ethnic groups (Varshney, 2002; Lehtsaar, 2015). While the source of the conflict may be political, social, economic, or religious, those individuals who are involved in such a conflict must expressly fight for the position of their ethnic group within the overall society. This criterion differentiates ethnic conflict from other forms of struggle. There is no commonly agreed explanation between scholars about what causes ethnic conflict. Rather, there are several competing and complementary hypotheses, each of which can be debated. Based on the vast amount of existing literature that covers ethnic conflict, we can point out the likelihood that confrontation between different groups is related to the following issues: discrimination, inequality, perceived injustice, a sense of danger, mistrust, exclusion from power, various and conflicting values, a lack of cultural awareness, and a lack of cultural empathy (see Katz, 1965; Kreidler, 1984; Moore, 2003; Eidelson & Eidelson, 2003; Cederman *et al,* 2011). However, there are a great many factors that are debated by scholars as an explanation for conflict, including the following: structural factors, such as weak or poorly-governed states (Fearon, 2011, Sambanis, 2004); weak territorial control (Lindemann, 2014); government repression (Lindemann, 2014; Hegre *et al,* 2001); population pressure, and a sudden shift in population size (Sambanis, 2001; Collier & Hoeffler, 2004; Fearon & Laitin, 2003);

including an unequal population size (Homer-Dixon, 2001), and the existence of a high proportion within that population of young males (Collier *et al,* 2006; Goldstone, 2001); globalisation (Ishiyama, 2004); a scarcity of resources or unequal access to valuable resources like oil and gas (Ross, 2004; Collier & Hoeffler, 2004; Lujala, *et al,* 2007); environmental scarcity (such as access to water) and climate change (Sirin, 2011; Brzoska & Fröhlich, 2016); an experience of prior conflict (Collier & Hoeffler, 2004; Vanhanen, 2012), or new technological means (such as that provided by the internet or social media) which fosters mobilisation (Cronin, 2006). However, what is mostly agreed upon is the conclusion that ethnic conflict is the result of mixed motivations (Bara, 2014; Carment, 2017) and opportunities (Collier, Hoeffler & Sambanis, 2005; Fuller *et al,* 2002).

Research into the field of ethnic conflict is accelerating at a tremendous speed, being fragmented and interdisciplinary. Despite the wide body of available research, however, there has been a lack of any systematic overview of the main arguments regarding the triggers behind ethnic conflict. So that it can provide an input (or some degree of value) for the scientific community in the field of ethnic conflict, this paper asks the following research questions: 1) what are the competing hypothesis for the reasons behind a conflict; and 2) what gaps in the research need to be addressed in the future to harmonise current understanding. Therefore, the goals of this paper are as follows: 1) to identify the central thematic aspects in literature that revolves around the subject of ethnic conflict; 2) to provide an overview of significant debates, highlighting those areas in which consensus has been achieved, and to uncover which aspects have not yet received enough attention in the available literature covering ethnic conflict or in existing empirical studies; and 3) to provide recommendations and directions for future research.

This paper has been assembled in a review format. It follows the general structure of a semi-systematic literature review (Snyder, 2019). Following the introduction, Section 2 presents the method being used here for literature mining, and identifies the main themes in that literature. Section 3 presents the results for the thematic literature analysis. In this section, I review the past and present research focuses, and existing hypotheses and theories. In Section 4, research gaps are explored and some guidance is provided for possible avenues to be taken in terms of future research. Finally, Section 5 concludes the study with a summary of the research and findings.

2. THE LITERATURE MINING PROCESS

To be able to establish a comprehensive collection of approaches to ethnic conflict, a search of English language publications was conducted, initially using the keywords 'ethnic conflict' and 'ethnic violence'. From these searches, new keywords emerged, such as 'horizontal inequalities' and 'ethnic grievances', which were additionally explored. Searchers were carried out through academic literature databases, such as Taylor & Francis, SAGE, JSTOR, and Google Scholar. I combined the full-text searches with those which listed only publications in which the terms were explicitly named as a major (sub-) topic in the title or in the abstract, and/or the publications in question focused on the determinants that trigger ethnic conflict based on theory or empirical country studies. In addition, relevant publications were identified as they were cited in the publications I scrutinised.

Although the review draws on schools of thought that have evolved over several decades, it emphasises the most-recent empirical findings. I limited my search to recent literature on ethnic conflict, published since 1990, because this is when ethnic conflict became a prominent issue for both academia and policymakers. Before the 1990s the question 'what causes ethnic violence?' was rarely asked (Toft, 2017), with few exceptions, such as Donald Horowitz (1985). Since the early 1990s, the collection of quantitative data that is based on case studies has made it possible to gain a better understanding of the triggers behind ethnic conflict.

The literature search resulted in around 620 results, mainly of peer-reviewed articles, books, and essays. Following a critical review of these results, about 96 relevant articles were chosen for the thematic literature review, all of which met the initial search criteria and provided sufficient input for the research questions.

Keyword analysis

The relevant literature, including most central or pivotal empirical research and theory on ethnic conflict, was synthesised in an inductive way by determining a set of relevant dimensions of ethnic conflict.

The dimensions were drawn from the keyword analysis, which has been indicated (above) by the authors in the articles. All of the keywords from a total of 96 articles were inserted into Nvivo 11 and analysed by word frequency (only stem words were used). This provided an understanding of the essential issues being discussed in the articles. Although there were also some minor topics, I focused on the main themes. The top ten most frequently-used keywords were compiled into Figure 1. The bigger the block in Fig 1, the more a word was found to be present in the keywords. For example, the keyword 'ethnic',* was counted a total of 95 times, while 'grievances' was counted fourteen times. Keywords, such as 'conflict', 'violence', 'war', 'civil', and 'political', were part of phrases, such as 'ethnic conflict', 'civil war', and 'political violence'. 'Ethnic' was also used for 'ethnicity'. Based on the results, I identified three thematic fields: 1) ethnicity and identity; 2) grievances and inequality; and 3) the presence of several ethnic groups.

KEYWORDS

<table>
<tr><td rowspan="3">ethnic</td><td rowspan="3">conflict</td><td>wars</td><td>political</td><td colspan="2">groups</td></tr>
<tr><td rowspan="2">civil</td><td rowspan="2">violence</td><td>identity</td><td rowspan="2">inequality</td></tr>
<tr><td colspan="2">grievances</td></tr>
</table>

FIGURE 1: The top ten most-used keywords as taken from the literature review (the chart has been drawn up using the Nvivo 11 program).

Based on the results of the keywords analysis, I will focus on three thematic areas. Firstly, ethnic group identities are a resource for mobilisation (Østby, 2008). Scholars argue that ethnicity provides a certain strategic opportunity for group mobilisation that can be used when fighting for economic and political goals (Fearon & Laitin, 2003; Kaufmann, 2005). Secondly, the competition of 'grievance' versus 'greed' schools of thought, which, firstly, suggests that ethnic conflict is more likely when ethnic groups suffer from (perceived) relative deprivation (Gurr, 2000) and,

secondly, a group of scholars argues for opportunity factors to be present so that a conflict may occur (Collier & Hoeffler, 2004; Fearon & Laitin, 2003). The third widely-observed aspect in the literature that covers ethnic conflict is the relative demographic size of one group in comparison with other groups within the state (Cederman *et al,* 2011; Posner, 2004), or the concentration of a group within a specific area of territory (Toft, 2003; Klašnja & Novta, 2016). This leads to the question of whether group polarisation or fractionalisation is a better indicator for measuring conflict. Different hypotheses regarding these issues are examined in detail in the following sub-sections.

3. THE RESULTS OF THE THEMATIC ANALYSIS

3.1. UNDERSTANDING 'ETHNICITY' IN ETHNIC CONFLICT

Ethnic conflict has been explained by means of various identity-related theories. The identity of social identity (Tjafel & Turner, 1979) and the related uncertainty-identity theory (Hogg, 2007) have both been used to explain why perpetrating violence on behalf of one's group is expected to increase identification with that group. Identity tends to be related to more deep-rooted values, such as one's sense of self-esteem and basic human needs; and threats to identity therefore produce a strong response. According to the uncertainty-identity theory, individuals identify with groups to reduce uncertainty about their self and their place in the world (Hogg, 2007). In addition, for those individuals who have fewer segments to their overall identity, identification strengthens in terms of the few identity segments they do have (Hogg & Adelman, 2013) and in contrast to others.

To be able to understand ethnic conflict, we must first understand the concept of ethnicity and what role it plays in mobilising groups. A good many studies do not differentiate between ethnicity and ethnic group (Vanhanen, 1999; Albert, 2014; Carment, 2017). People who share ethnic traits do not automatically constitute an ethnic group, however. People must consciously acknowledge that they belong to a group (Tajfel & Turner, 1986), such as in terms of identifying themselves with in-group members and distinguishing themselves from non-group ('out-group') members. A sense of collective belonging may include markers that are based on common descent, language, religion, race, or history, or a combination of these (Fearon, 2006; Horowitz, 1985; Wimmer, 2013; Gundelach & Manatschal, 2017). There are numerous descent-based attributes, but only a few of them become socially and politically relevant. In the past few decades there has been a sharp increase in violent sectarian or religious tensions, ranging from Islamic extremists waging global jihad, to the persecution of Rohingya Muslims in Myanmar, and outbreaks of violence between Christians and Muslims in Egypt (Kishi, 2018). Religious boundaries are often argued to incite violence

(Reynal-Querol, 2002; Fox, 2000) and, as religious identities are particularly salient for individuals, this makes conflict resolution difficult (Toft, 2007; Wellman & Tokuno, 2004).

In addition, language can become a key in-group/out-group marker (Smirnova & Iliev, 2017) and a tool for discrimination (Gluszek & Dovidio, 2010). However, conflicts that are based on language divisions have showed mixed results when it comes to their being covered by empirical studies. For example, Collier & Hoeffler (2004) and Fearon & Laitin (2003) did not find any link between language and intergroup violence, concluding that linguistic divides may ease peaceful political solutions. Laitin (2007, p 59) makes the point that language is not exclusive, unlike religion and race; individuals can learn an additional language without changing their beliefs or identities. If so, armed conflict should be relatively rare when ethnic groups are mobilised based on linguistic boundaries (Laitin, 2000; Rørbæk, 2017). Furthermore, the dataset which covers Ethno-Linguistic Fractionalisation (ELF) (Reyna-Querol, 2002), which coded linguistic groups, was harshly criticised for its use when explaining political conflict because language cannot be an autonomous factor in explaining conflict. Other scholars, such as Montalvo & Reynal-Querol (2005), found a positive and statistically significant effect between intergroup violence and ethnolinguistic polarisation.

The idea that we can identify and categorise people and place them in certain groups is still open to debate. The disagreement about the role of ethnicity in the onset of conflict stems from a more fundamental debate over whether ethnic identity is even a meaningful category in terms of understanding group behaviour, or whether these identities are (re) created and instrumentalised by leaders to create conflict so that they can grasp political or economic power (Watts *et al,* 2017). For example, research by Jakobsen et al (2016) supports the argument that conflicts which are taking place along ethnic lines are not caused primarily by primordial hatred between different ethnic groups, but that they indicate the possibility that ethnicity may be used as an instrument to create violent conflict. That argument is supported by Jenne et al (2007), who concluded that ethnicity can provide leaders with the strategic leverage needed for recruiting group members to fight for a cause or, as other authors found, can be used as an instrument to retain power and control (Gagnon, 2000; Snyder, 2000).

On the other hand, Cederman & Wucherpfennig (2017) highlight their finding that ethnic conflicts are typically about 'nationality problems' of self-rule and are driven by political and economic inequalities between groups. Bhavnani and Miodownik (2008, p 45) also find that ethnicity is a key determinant of conflict if individuals are attached to their ethnic identities and, therefore, ethnic salience should take centre stage in explanations that attempt to forge a link between ethnicity and conflict. Some authors argue that ethnicity will increase the likelihood of conflict (as a secondary effect) if group-belonging becomes the basis for determining political and socio-economic access and control (Gurr, 1970; Wimmer *et al,* 2009), or if it is territory-based and has secessionist and/or separatist demands (Toft, 2002). Some authors see the likelihood of ethnic conflict reoccurring if conflict has existed previously between the involved groups. Mattes & Savun (2009, p 754) point out that conflicts with an ethnic component are nearly twice as likely to reoccur. Ethnicity is believed to intensify conflict according to some studies (Costalli & Moro, 2011; Montalvo & Reynal-Querol 2005; Weidmann, 2011), but in others this correlation has not held true. For example, Klašnja and Novta (2016) demonstrated that in highly ethnically-polarised societies, increased ethnic segregation served to decrease the incidence and intensity of conflict. Korostelina (2008) in her research looked into the formation process of national identity and showed that in Crimea, the civic concept of national identity significantly reduced the readiness for conflict amongst ethnic minorities; and the position of a minority within the nation regulated the readiness to fight with other groups.

Albert (2014) makes the case that ethnic group identity has substantial effects on collective action, particularly violent conflict, and a mechanism must exist to predict behaviour so that ethnic group identity can be properly measured. For that purpose he created a measurement for ethnic group identity - the Ethnic Group Identity Index (EGII). Although ethnicity is a convenient and salient marker when it comes to identifying a particular conflict as an ethnic conflict, its deeper role in mobilising different groups is still up for discussion.

3.2. THE ROLE OF GROUP GRIEVANCES IN ETHNIC CONFLICT

The second dilemma that is central to the literature covering ethnic conflict – and something that has divided scholars of intrastate conflict for decades – is the 'grievance' versus 'greed' factors as a cause of conflict. Scholars question whether violent conflict is more likely when an ethnic group suffers from perceived or real grievances, or could conflicts be the product of an environment in which conflict can thrive? The 'grievance' school of thought relies largely on the relative deprivation theory that was formulated by Gurr (1970) in the 1970s. Gurr's theory is based on the concept that individuals may feel deprived of some desirable object or item that is relevant to their own past, or to other individuals or groups, or to some other form of social category (Walker, & Pettigrew, 1984). He highlighted political and socio-economic inequalities as motivational forces behind ethnic conflict. When there is a gap between the expectations of certain values and the capability of being able to obtain and maintain them, this creates grievances and feelings of injustice, which in turn may lead to an increase in the level of frustration and then to violent conflict. Literature regards the psychological factors of relative deprivation and frustration as a major force behind violent actions. The experiment by Shaykhutdinov & Bragg (2011) highlighted the relationship between frustration and conflict: when participants feel their autonomy and ability to express their group identity is seriously threatened, they are more likely to choose protest over negotiation.

The debate regarding 'greed' or opportunity factors in an intergroup conflict was ignited by Collier & Hoeffler (2004), who suggested that conflict is driven either by greed or grievances. They questioned the grievance-based approach because those situations in which people want to rebel are ever-present, and just inequalities cannot explain the reasons behind such conflict. In other hand, they found that opportunity factors in which people can rebel are quite rare when it comes to their constituting an explanation for conflict (Bara, 2014). Collier & Hoeffler (2004) showed that economic incentives (the opportunity to loot) are the main reasons for violent conflict. This argument was supported by research by Fearon & Laitin (2003) in which they concluded that the risk of conflict lies rather in the conditions that favour rebellion, such as poverty, a weak state, and political instability. Earlier work by Collier & Hoeffler is still

widely cited today, and a large number of country studies are therefore based on their greed theory, while excluding the grievance factors.

Despite the popularity of the work of Collier & Hoeffler, subsequent empirical studies and statistical modelling have shown that conflict involves a more complex interplay of incentives and opportunity factors (Goodhand, 2003; Ballentine & Sherman, 2003, pp 6; Korf, 2005, pp 201-202; Østby, 2008; Sambanis, 2005, pp 329; Brown, 2009; Østby *et al,* 2011; Kruglanski *et al,* 2009; Monahan, 2012; Saucier *et al,* 2009; Lindemann, 2014; Hillesund *et al,* 2018). For example, Lindemann (2014) developed a nine-factor model of ethnic conflict (involving four grievances and five opportunity factors) study conflict trajectories in similar ethnic groups (the Kurds in Turkey and Syria). Stewart (2002) came up with the horizontal inequality concept, which provides an explanation both for the motive and opportunity required for people to engage in violence. Even Collier & Hoeffler, based upon their research on sixteen case studies, later abandoned the either/or argument and agreed that more complex models which consider greed and grievance together as motives for violent conflict should instead be used (Collier, Hoeffler, & Sambanis, 2005).

3.3. DEMOGRAPHIC ASYMMETRY: DOES GROUP SIZE MATTER?

An important prerequisite for the emergence of intergroup conflict that comes up in literature covering ethnic conflict is the ability of groups to rally their members around a common goal, including generating a readiness to act on behalf of the group (Olson, 1965; Østby, 2008; Østby *et al,* 2009, Kustov, 2017; Stewart, 2008). Group size and territorial concentration indicate a group's capacity to mobilise (Weidmann, 2009; Toft, 2002). Small groups may not be able to gather together enough resources (such as money, weapons, or skills, for instance), and groups that scattered far and wide may face problems in coordination (Bara, 2014). This, however, does not mean that small groups cannot interrupt societal peace. Instead, they may simply turn to non-traditional tactics, such as terrorism or rebellion to, cope with the problems raised by asymmetry (Sambanis & Shayo, 2013; Cook & Olsen Lounsbery, 2017; Ghatak, *et al,* 2019).

Most scholars have found that the risk of intrastate violence decreases or is negatively correlated in highly homogeneous and highly diverse societies (Horowitz, 1985; Collier & Hoeffler, 2004; Reynal-Querol, 2002; Ellingsen, 2000; Fearon & Laitin, 2003; Østby *et al,* 2009; Costalli & Moro, 2011). For example, Costalli & Moro (2011) found empirical support for the claim that in those areas in which one group was dominant – i.e. where they formed at least 75 per cent of the total population of a municipality, or where they formed the second-largest ethnic group but did not exceed 20 per cent of the total population – the level of violence was lower. Dominant groups are usually less motivated to pick up arms, as they already hold power and privilege in such a society and, in contrast, marginalised groups lack the resources. Therefore, for dominant groups to be able to take part in violent conflict, they should be motivated by factors, such as fear that their privilege is about to be taken away, or by a more aggressive desire to dominate other groups (Stewart, 2002). Wegenast & Basedau (2014), however, showed that this is not always the case, and found that in certain circumstances, high levels of ethnic diversity could be a potential risk factor in terms of conflict. In their study, oil provided an incentive for marginalised groups to overcome the collective action problem.

The risk of ethnic conflict has mostly been associated with high levels of polarisation. Polarisation is at its highest when a society is composed of two equally-sized ethnic groups. The probability is of violence being more prone to erupt in an environment in which exists two groups of approximately the same size with opposing goals, rather than in an environment in which a number of small groups is present, or one single dominant group. This was first illustrated by Horowitz (1985) and Esteban & Ray (1994), but was subsequently supported by the work of other scholars (see, for example, Hegre, 2008; Schneider & Wiesehomeier, 2008; Bhavnani & Miodownik, 2008; Cederman & Girardin, 2007; Montalvo & Reynal-Querol, 2005; Collier & Hoeffler, 2004; Ellingsen, 2000). Ellingsen (2000) proved in her research that in countries in which the population share of the dominant group is less than eighty per cent, intrastate conflict is more frequently experienced than it is in more homogeneous countries. The model by Collier and Hoeffler (2004) showed that societies in which the largest ethnic group forms 45 per cent and ninety per cent of the population total have around double the risk of conflict. Presumably this is because such societies have both the power and the incentive to exploit their minorities.

A similar threshold has been used by Jakobsen et al (2016), who suggested that each group must constitute at least 35 per cent of the total population for its members to feel safe. If this level is lower, individuals will feel that their group's position, culture, ethnicity, or status is threatened. They argued that in every society there is a turning point of tolerance, i.e. up to a certain point intergroup contact will increase tolerance, and after the level is reached, any further diversity will lead to less tolerance.

The negative effect of new residents or a sudden immigration influx in the attitudes of natives has also been shown in other studies (see Karreth *et al,* 2015; Meuleman *et al,* 2009; Putnam, 2007). Spain (1993) explained that when the number of new residents reaches critical mass, and when resources are reallocated and subsequently privatised, conflicts over values and the definitions of community eventually ensue between 'been-heres' and 'come-heres'. Outsiders create conflict when they reach a critical mass that allows them to turn the community to their own advantage. To avoid this, Singapore has set a quota for non-Malaysian households at five per cent in a specific neighbourhood and at eight per cent in a block (Non-citizens..., 2019).

High polarisation has been quite an accurate predictor for conflict, along with the duration of conflict (Montalvo & Reynal-Querol, 2005), and the severity of the ensuing violence. Costalli & Moro (2011) concluded in their essay that four municipalities which belonged to the list of the ten most polarised areas in Bosnia-Herzogovina during 1992–1995 were also included in the list of the ten most violent municipalities, while none of the ten most diverse municipalities appeared in such a list. Subsequently, research by Kustov (2017) challenged preceding arguments that polarisation increases conflict. Contrarily, his computational analysis suggested the opposite. He showed that there is no 'most hazardous' ethnic structure *per se* and both polarisation and cross-cuttingness appear to decrease the likelihood of conflict, but also to increase the potential intensity of conflict.

Therefore, conflict is not simply a function of group size alone. Recent studies have demonstrated that it is not only high levels of polarisation that makes conflict more likely, but that segregation and polarisation jointly determine the spread of any conflict (see Lim *et al,* 2007; Klašnja & Novta, 2016). Klašnja & Novta (2016) proved in their research that

for highly ethnically polarised societies, increasing ethnic segregation decreased the incidence and intensity of conflict. In contrast, in societies with low ethnic polarisation, increasing segregation increases conflict.

4. RESEARCH GAPS AND FURTHER RESEARCH NEEDS

Some of those research gaps and dilemmas that I was able to identify in the thematic literature are now summarised below:

4.1. ETHNICITY

Although substantial areas of general knowledge have been accumulated to explain the role of ethnic identity in mobilising groups towards committing violent action, there is still little to be known about the processes that link identity, leadership, and mobilisation (Gurr, 2017). As mentioned above, is identity a mean or is it a reason for collective action? What is the relationship between ethnicity as a concept and the likelihood, frequency, or intensity of identity-based conflict?

Furthermore, although, there are studies in existence that focus on different ethnic markers (such as language, religion, or origins), and on conflict, some scholars argue that different ethnic markers are not unique and a more general concept of ethnicity should be adopted, one which treats various ascriptive markers as being functionally equivalent (Rørbæk, 2017). As different ethnic markers are valid in different societies, the process of finding a common salient ethnic marker that is comparable in cross-national studies becomes a more difficult exercise. From this point of view, I would question first whether the role of different markers is so essential, or is the understanding of how strongly people identify with their group and how their behaviour can lead to mobilisation instead the central argument when it comes to understanding ethnic conflict? This line of research has already been started by Albert (2014) with his EGII, which seeks to measure the strength of ethnic group identity. Continuing empirical research on the role of ethnicity in terms of conflict would address these dilemmas.

4.2. PERCEIVED GRIEVANCES

One aspect that has not been at the forefront in the existing grievance literature and in previous empirical studies is group perception. The link between objective grievances and perceived grievances has been considered only in few studies. However, for example, objective inequalities cannot automatically be translated into perceived inequality. Therefore, the concept of grievances is subject to misperceptions and manipulation (Must, 2016). It becomes clear that researchers must keep in mind the thought that for conflict to break out, it is not enough that group members perceive inequality between groups; they must also come to find the situation unjust (Cederman, *et al,* 2013; Must, 2016). Miodownik & Nir (2016), in their cross-national comparative multilevel analyses of the Afrobarometer dataset, are able to confirm that subjective perceptions both amplify the effect of exclusion when it comes to the acceptance of violence and also alter the readiness towards dissent for those groups that are included. Although, research on the role of perceived inequality measures is somewhat sparse, with only limited geographical coverage (mainly covering African countries), it should not be overlooked.

4.2.1. Micro-level data versus macro-level data

The previous section highlights another weakness in the 'grievance' versus 'greed' literature: most of the empirical research is based on national (average) data, which explains the macro-level results using arguments that essentially operate at the micro level. Conflicts usually start and thrive at the local level, which is why only country-level measures, such as the Gin coefficient which measures income distribution amongst individuals (Cederman *et al,* 2011; Collier & Hoeffler, 2004; Hegre, 2008; Halika *et al,* 2020), the use of the unemployment rate to measure poverty levels (Halika *et al,* 2020), the use of national statistics and GIS data to measure population size and distribution (Cederman, *et al,* 2011; Klašnaja & Novta, 2016), all of which have been used by several scholars, fail to capture the motivations behind any conflict in terms of individual groups. I would therefore tend to be cautious when it comes to building up theories and research using variables that are based on country averages, as they do not capture the perceptions of group grievances which serve as a formidable tool for recruitment (Cederman *et al,* 2011). More attention must be given to linking data in regards to objective variables to data on

the perceived grievances of individuals or groups. In my mind, perceptual mechanisms are important where they can be used to understand group behaviour. People often act in terms of a socially-mediated understanding of their conditions, rather than in terms of the conditions themselves. Perceptions breed discontent and discontent leads to aggression.

It would therefore be irresponsible to dismiss the role of grievances in ethnic conflict studies; and more theoretical and empirical research at the meso-level and micro-level, using more sophisticated measures, should be favoured to revive the importance of grievance hypothesis in ethnic conflict literature. In understanding this problem, several scholars (such as Buhaug *et al,* 2009; Cunningham & Weidmann, 2010; Costalli & Moro, 2011; Rustad *et al,* 2011; Hillesund *et al,* 2018) have recently abandoned traditional cross-country analyses to focus instead on disaggregated data and internal diversity. They have also focused on variables that can be measured at the sub-national level (Halika *et al,* 2020; Hegre *et al,* 2019). Therefore, I agree with those authors who recommend taking the next step both in terms of the dynamics behind violent and non-violent ethnic conflict, and prioritising research at the local level (Hillesund *et al,* 2018; Stroschein, 2017; Jenne, 2017), or even going down to the individual level to properly investigate the micro-level mechanisms that are at play (Hillesund *et al,* 2018).

4.3. GROUP POLARISATION

The measure of society's polarisation is seemingly more theoretical than making use of its diversity and dominance, in terms of relative group size when compared to the rest of the groups in the territory, meaning that it is more relevant than simply noting the presence of several groups within a given area of territory. However, even if high levels of polarisation have been quite a good indicator for predicting ethnic conflict, the empirical evidence is mixed. Besides Kustov, some other studies do not explicate the correlations and, in some cases, the findings appear not to be empirically robust (Forsberg, 2008). Some authors (Caselli & Coleman, 2013; Bhavnani & Miodownik, 2008) point out that the summary statistics that have been used in previous studies (such as Fearon & Laitin 2003; Collier & Hoeffler 2004; Montalvo & Raynal-Querol, 2005) take the existing

ethnic structure of the population as being exogenous or assumes that ethnic salience is constant across individuals. This assumption, however, may lead to incorrect conclusions. Following this argument, Caselli & Coleman (2013) built their model on the prediction that relative group sizes change in response to conflict (such as when a defeated group joins the dominant one). Bhavnani & Miodownik (2008) also showed in their models that the results are different when ethnicity is a 'fixed salience', meaning that when salience was fixed, the onset of conflict was twice as likely at low levels of polarisation when compared to instances in which salience is permitted to vary, with the difference decreasing at high levels of polarisation.

The literature review showed the evolution of research on the correlation of simple group sizes and the risk of ethnic violence. While, in the middle of the 1980s, Horowitz showed that moderately diverse societies are more prone to conflict, recent empirical studies have failed to offer complete support for that hypothesis. Recent studies (see, for example, Kustov, 2017; Caselli & Coleman, 2013; Bhavnani & Miodownik, 2008) have pointed towards the weaknesses of polarisation as a variable when it comes to predicting conflict. Further empirical research, testing, and verification of the different variables, including population size, should therefore be addressed to discover an answer to the eternal question: in which kind of population setting is ethnic conflict most likely to be triggered?

CONCLUSIONS

The aim of this paper was to review the available literature on ethnic conflict to be able to distil the essential elements of the phenomena and to provide a roadmap when it comes to being able to navigate through the vast body of available literature and arguments regarding the essence of ethnic conflict. This review summarised the main themes and hypotheses, and explored gaps in the current research, while focussing on three essential elements that are widely discussed in the available conflict literature. These elements were drawn up using the keyword analysis: understanding what role is played in ethnic conflict by ethnicity, (perceived) grievances, and opportunities; and what role is played by a group's population size.

The growing body of empirical research over the past few decades has shown that few, if any, scholars have attached any importance to mono-causal explanations of ethnic conflict. There is a strong body of support for the assumption that mixed motivations facilitate conflict. What this mix may consist of, however, is still an open question. Hopefully, further empirical research will help to strengthen the arguments, and statistically prove the relevance of various conflict variables (such as poverty, a weak state, feelings of discrimination, or inequality, or trust, limited resources, or population size), and through this explain which aspects may play a role in causing ethnic conflict. Current arguments and hypotheses are controversial. This has largely to do with different methodologies and datasets that are being used by scholars, while the limited number of regional studies (which focus mainly on African countries) do not provide a comprehensive body of knowledge which would make it possible to build up new theories or understanding regarding the triggers of ethnic conflict. I therefore have to conclude that the theories and techniques used in the available studies require further development and common areas. I can expect to find that many of the gaps that I have highlighted in this literature review could be further researched, especially those that are related to quantitative research on ethnic conflict at the sub-national level, along with the role of group perception in terms of mobilisation, and what role ethnicity plays in any given conflict. Growing empirical studies are definitely leading us towards greater research clarity, which is something that is very much needed to be able to expand the currently-polarised theoretical background.

DISCLOSURE STATEMENT

No potential conflicts of interest were reported by the author.

Contact:

Helina Maasing
E-mail: helina.maasing@mail.ee

REFERENCES AND SOURCES

Albert, C. D. (2014). 'The ethno-violence nexus: measuring ethnic group identity in Chechnya'. *East European Politics*, 30:1, pp. 123-146. Available at: DOI: 10.1080/21599165.2013.848796

Ballentine, K. & Sherman, J. (2003). 'Introduction'. In: Karen Ballentine & Jake Sherman (eds.) *The Political Economy of Armed Conflict: Beyond Greed and Grievance*. Boulder, CO: Lynne Rienner, pp. 1–15.

Bara, C. (2014). 'Incentives and opportunities: A complexity-oriented explanation of violent ethnic conflict'. *Journal of Peace Research*, Vol. 51(6) pp. 696–710.

Bhavnani, R. & Miodownik, D. (2008). 'Ethnic polarization, ethnic salience, and civil war'. *Journal of Conflict Resolution*, Vol. 53(1) pp. 30–49.

Brown, G. K. (2009). 'Regional autonomy, spatial disparity and ethnoregional protest in contemporary democracies: A panel data analysis, 1985–2003'. *Ethnopolitics,* Vol. 8(1), pp. 47–66.

Brzoska, M & Fröhlich, C. (2016). 'Climate change, migration and violent conflict: vulnerabilities, pathways and adaptation strategies'. *Migration and Development*, Vol. 5:2, pp. 190-210, Avalilable at: DOI: 10.1080/21632324.2015.1022973

Buhaug, H., Gleditsch, K. S., Holtermann, H., Østby, G. & Tollefsen, A. F. (2009). 'Revolt of the paupers or the aspiring? Geographic wealth dispersion and conflict'. Unpublished manuscript, *Centre for the Study of Civil War,* PRIO.

Carment, D. (2017). 'Old Wine, New Bottles: Synthesis and Integration in Ethnic Conflict Research'. *Ethnopolitics*, Vol. 16:1, pp. 98-105, Available at: DOI: 10.1080/17449057.2016.1235825

Caselli, F. & Coleman II, J W. (2013). 'On the Theory of Ethnic Conflict'. *Journal of the European Economic Association*, Vol. 11, Supplement 1: 10 thAnniversary Celebratory Issue, pp. 161-192. Published by: Oxford University Press.

Cederman, L-E. & Girardin, L. (2007). 'Beyond fractionalization: Mapping ethnicity onto nationalist insurgencies'. *American Political Science Review,* Vol. 101(1) pp. 173–185.

Cederman, L-E., Weidmann, N. B & Gleditsch, K. S. (2011). 'Horizontal Inequalities and Ethnonationalist Civil War: A Global Comparison'. *American Political Science Review* Vol. 105(3), pp. 478–495.

Cederman, L-E., Gleditsch, K.S. & Buhaug, H. (2013). *Inequality, Grievances, and Civil War.* Cambridge: Cambridge University Press.

Cederman, L-E. & Wucherpfennig, J. (2017). 'Inequalities Between Ethnic Groups, Conflict, and Political Organizations'. *Ethnopolitics*, Vol. 16:1, pp. 21-27, Available at:10.1080/17449057.2016.1235342

Collier, P., & Hoeffler, A. (2004). 'Greed and grievance in civil war'. *Oxford Economic Papers*, Vol. 56, pp. 563-595.

Collier, P., Hoeffler, A. & Sambanis, N. (2005). 'The Collier–Hoeffler model of civil war onset and the case study project research design.' In: Collier, P. & Sambanis, N. (eds), *Understanding Civil War: Evidence and Analysis*. Washington, DC: World Bank.

Collier, P., Hoeffler, A. & Rohner, D. (2006). 'Beyond Greed and Grievance: Feasibility and Civil War'. *CSAE* WPS/2006–10, Oxford, UK: University of Oxford.

Costalli, S. & Moro, F. N. (2011). 'The patterns of ethnic settlement and violence: a local-level quantitative analysis of the Bosnian War'. *Ethnic and Racial Studies*, Vol. 34:12, pp. 2096-2114, Available at: DOI: 10.1080/01419870.2011.556748

Cook, A. H. & Olson Lounsbery, M. (2017). 'Conflict Dynamics: A Comparative Framework' In: *Conflict Dynamics: Civil Wars, Armed Actors, and Their Tactics*. Published by: University of Georgia Press.

Cronin, A. K. (2006). 'Cyber-Mobilization: The New Levée en Masse'. *Parameters*, Summer 2006, pp. 77–87.

Cunningham, K. & Weidmann. N. (2010). 'Shared Space: Ethnic Groups, State Accommodation, and Localized Conflict'. *International Studies Quarterly,* Vol. 54, pp. 1035-54.

Ellingsen, T. (2000). 'Colorful Community or Ethnic Witches' Brew? Multiethnicity and Domestic Conflict During and After the Cold War.' *The Journal of Conflict Resolution*, Vol. 44(2), pp. 228-249.

Fearon, J. D. & Laitin, D. (2003). 'Ethnicity, Insurgency, and Civil War'. *American Political Science Review*, Vol. 91, pp. 75-90.

Fearon, J. D. (2006). 'Ethnic mobilization and ethnic violence'. In: Weingast, B.R & Wittman D.A. (eds). *The Oxford Handbook of Political Economy. Oxford*: Oxford University Press, pp. 852–868.

Fearon, J. D. (2011). 'Self-Enforcing Democracy'. *Quarterly Journal of Economics*, Vol. 126(4), pp. 1661–1708.

Forsberg, E. (2008). 'Polarization and Ethnic Conflict in a widened strategic setting'. *Journal of Peace Research*, Vol. 45 (2), pp. 283-300.

Fox, J. (2000). 'The ethnic-religious nexus: The impact of religion on ethnic conflict'. *Civil Wars,* Vol. 3:3, pp. 1-22, Available at: DOI: 10.1080/13698240008402444

Fuller, G. A., Morrison, R., Murphy, A. B. & Ridgley, M. (2002). 'Potential for Ethnic Conflict in China'. *Eurasian Geography and Economics*, Vol. 43:8, pp. 583-609, Available at: DOI: 10.2747/1538-7216.43.8.583

Gagnon, V. P. (2000). 'Spiraling to Ethnic War'. *International Security*, Vol. 2(21)

Ghatak, S., Gold, A., & Prins, B. C. (2019). 'Domestic Terrorism in Democratic States: Understanding and Addressing Minority Grievances'. *Journal of Conflict Resolution*, Vol. 63(2), pp. 439-467.

Gluszek, A., & Dovidio, J. F. (2010). 'The way they speak: A social psychological perspective on the stigma of non-native accents in communication.' *Personality and Social Psychology Review*, Vol, 4, pp. 214-237.

Goldstone, J. (2001). 'Demography, Environment and Security: An Overview'. In Myron Weiner, M. & Stanton Russell, S. (eds.), *Demography and National Security*, New York: Berghahn Books, pp. 38–61.

Goodhand, J. (2003) 'Enduring Disorder and persistent poverty: a review of the linkages between war and chronic poverty'. *World Dev*; No. 31 pp. 629-46.

Gundelach, B., & Manatschal, A. (2017). 'Ethnic Diversity, Social Trust and the Moderating Role of Subnational Integration Policy'. *Political Studies*, Vol. 65(2), pp. 413– 431.

Gurr, T. R. (1970). *Why Men Rebel*. Princeton, NJ: Princeton University Press

Gurr, T. R. (2000). *Peoples Versus States: Minorities at Risk in the New Century*. Washington, DC: United States Institute of Peace Press.

Gurr, T. R. (2017). 'Observations on the Study of Ethnic Conflict'. *Ethnopolitics*, Vol. 16:1, pp. 34-40, Available at: DOI: 10.1080/17449057.2016.1235345

Eidelson, R. J. & Eidelson, J. (2003). 'Dangerous ideas: five beliefs that propel groups toward conflict'. *American Psychologist*, Vol. 58: pp. 182–192.

Halika, M., Ferri, S., Schellens, M. K., Papazoglou, M. & Thomakos, D. (2020). 'The Global Conflict Risk Index: A quantitative tool for policy support on conflict prevention.' *Progress in Disaster Science, No.* 6, 100069

Hegre, H., Ellingsen, T., Gates, S. & Gleditsch, N. S. (2001). 'Toward a Democratic Civil Peace? Democracy, Political Change, and Civil War, 1816–1992'. *American Political Science Review,* Vol. 95 (1), pp. 33–48.

Hegre, H. (2008). 'Polarization and Interstate Conflict'. *Journal of Peace Research*, Vol. 45 (2), Special Issue on Polarization and Conflict, pp. 261-282

Hegre H, Allansson M, Basedau M, Colaresi M, Croicu M, Fjelde H, et al. (2019). 'ViEWS: a political violence early-warning system'. *Journal of Peace Research*, Vol. 56(2), pp. 155–174 Available at: DOI: 10.1177/0022343319823860

Hillesund, S., Bahgat, K., Barrett, G., Dupuy, K., Gates, S., et al. (2018). 'Horizontal inequality and armed conflict: a comprehensive literature review'. *Canadian Journal of Development Studies / Revue anadienne d'études du développement*, Vol. 39:4, pp. 463-480, Available at: DOI: 10.1080/02255189.2018.1517641

Hogg, M.A. (2007). 'Uncertainty-identity theory'. In: Zanna MP (eds.) *Advances in experimental social psychology*, Vol. 39. Academic Press, San Diego, pp 69–126.

Hogg, M & Adelman, J. (2013). 'Uncertainty–Identity Theory: Extreme Groups, Radical Behavior, and Authoritarian Leadership'. *Journal of Social Issues*, Vol. 69, No. 3, pp. 436–454.

Homer-Dixon, T. F. (2001). Environment, Scarcity, and Violence, Princeton, N.J.: Princeton University Press.

Horowitz, D. (1985). *Ethnic Groups in Conflict*. Berkeley, CA: University of California Press.

Ishiyama, J. (2004). 'Does Globalization Breed Ethnic Conflict?' *Nationalism and Ethnic Politics*, Vol. 9:4, pp.1-23, Available at: DOI: 10.1080/13537110390444078

Jakobsen, T. G., Vogt Isaksen, J., Skavhaug, G.K. O. & Anderssen Bakkan, H. (2016). 'The Turning Point of Tolerance'. *International Journal on Minority and Group Rights*, Vol. 23 (1), pp. 80-104.

Jenne, E., Saideman, S. & Lowe, W. (2007). 'Separatism as a Bargaining Posture: The Role of Leverage in Minority Radicalization'. *Journal of Peace Research*, Vol. 44 (5), pp. 539–558.

Karreth, J., Singh, S. P. & Stojek, S. M. (2015). 'Explaining Attitudes toward Immigration: The Role of Regional Context and Individual Predispositions'. *West European Politics*, Vol. 38:6, pp. 1174-1202, Available at: DOI: 10.1080/01402382.2015.1022039

Katz, D. (1965). 'Nationalism and strategies of international conflict resolution'. H. C. Kelman (eds.), *International behavior: a social psychological analysis* (pp. 356–390). New York: Holt, Rinehart & Winston.

Kishi, K. (2018). 'Key findings on the global rise in religious restrictions'. *Pew Research Center*, June 21, 2018.

Klašnaja, M., & Novta, N. (2016). 'Segregation, Polarization, and Ethinic Conflict'. *Journal of Conflict Resolution*, Vol 60(5), pp. 927-955.

Kaufmann, S. (2005). Rational Choice and Progress in the Study of Ethnic Conflict: A Review Essay. *Security Studies*, Vol. 14, No. 1, pp. 178–207.

Korf, B. (2005). 'Rethinking the greed–grievance nexus: Property rights and the political economy of war in Sri Lanka'. *Journal of Peace Research*, Vol.42(2), pp. 201–217.

Korostelina, K. (2008). 'Concepts of national identity and the readiness for conflict behaviour'. *National Identities*, Vol. 10:2, pp. 207-223, Available at: DOI: 10.1080/14608940801999131

Kruglanski, A., Chen, X., & Dechesne, M. (2009). 'Fully committed: Suicide bombers´ motivation and the quest for personal significance'. *Political Psychology,* Vol. 30(3), pp. 331–357.

Kustov, A. (2017). 'How ethnic structure affects civil conflict: A model of endogenous grievance'. *Conflict Management and Peace Science*, Vol. 34(6), pp. 660–679.

Laitin D. D. (2000). 'Language conflict and violence: The straw that strengthens the camel's back'. *European Journal of Sociology,* Vol. 41(1), pp. 97–137.

Laitin, D. D. (2007). *Nations, States, and Violence.* Oxford: Oxford University Press.

Lehtsaar, T. (2015). *Suhtlemiskonflikti psühholoogia*. Tartu: Tartu Ülikooli Kirjastus.

Lim, M., Metzler, R., & Bar-Yam, Y. (2007). 'Global pattern formation and ethnic/cultural violence'. *Science*, No. 317(5844), pp. 1540-1544.

Lindemann, S. (2014). Explaining divergent responses to ethnic exclusion: evidence from two paired comparisons. *Conflict, Security & Development*, Vol. 14(2), pp. 181-211.

Lujala, P., Rød, J. K. & Thieme, N. (2007). 'Fighting over oil: Introducing a new dataset'. *Conflict Management and Peace Science,* Vol. 24(3), pp. 239–256.

Mattes, M. & Savun, B. (2009). 'Fostering peace after civil war: Commitment problems and agreement design'. *International Studies Quarterly,* Vol. 53(3), pp. 737-759.

Meuleman, B., Davidov, E., & Billiet, J. (2009). 'Changing attitudes toward immigration in Europe, 2002–2007: A dynamic group conflict theory approach'. *Social Science Research*, Vol. 38(2), pp. 352–365.

Miodownik, D. & Nir, L. (2016). 'Receptivity to Violence in Ethnically Divided Societies: A Micro-Level Mechanism of Perceived Horizontal Inequalities'. *Studies in Conflict and Terrorism,* Vol. 39 (1), pp. 22–45.

Monahan, J. (2012). 'The individual risk assessment of terrorism'. *Psychology, Public Policy and Law,* Vol.18(2), pp. 167–205.

Montalvo, J. G. & Reynal-Querol, M. (2005). 'Ethnic polarization, potential conflict, and civil wars.' *American Economic Review,* Vol. 95(3), pp. 796–813.

Moore, C. W. (2003). *The mediation process: practical strategies for resolving conflict*. San Francisco, CA: Jossey-Bass.

Must, E. (2016). 'When and How Does Inequality Cause Conflict? Group Dynamics, Perceptions and Natural Resources'. *PhD thesis*, Department of Government, London School of Economics.

'Non-Citizen (NC) Quota for the Renting Out of Flat'. Retrieved from: https://services2.hdb.gov.sg/webapp/BR12AWNCQuota/

Olson, M. (1965). *The Logic of Collective Action*. Cambridge, MA: Harvard University.

Østby, G. (2008). ‹Polarization, horizontal inequalities and violent civil conflict›. *Journal of PeaceResearch,* Vol. 45(2), pp. 143–162.

Østby, G, Nordas, R. & Rød, J.K. (2009). ‹Regional inequalities and civil conflict in Sub-Saharan Africa.› *International Studies Quarterly,* Vol. 53, pp. 301–324.

Østby, G., Urdal, H., Tadjoeddin, Z. M., Murshed, M. S. & Strand, H. (2011). ‹Population pressure, horizontal inequality and political violence: A disaggregated study of Indonesian provinces, 1990–2003›. *Journal of Development Studies,* Vol. 47(3), pp. 377–398.

Posner, D. N. (2004). 'The political salience of cultural difference: Why Chewas and Tumbukas are allies in Zambia and adversaries in Malawi'. *American Political Science Review*, Vol. 98(4), pp. 529–545.

Putnam, R. D. (2007). 'E Pluribus Unum: Diversity and Community in the Twenty-First Century – the 2006 Johan Skytte Prize Lecture'. *Scandinavian Political Studies*, Vol. 30 (2), pp. 137–74.

Reynal-Querol, M. (2002). 'Ethnicity, political systems, and civil wars'. *Journal of Conflict Resolution,* Vol. 46(1), pp. 29–54.

Ross, M. (2004). 'How Do Natural Resources Influence Civil War? Evidence from Thirteen Cases'. *International Organization*, Vol. 58, pp. 35–67.

Rørbæk, L. L. (2017). 'Killing in the name of …? Types of ethnic groups and armed conflict.' *Cooperation and Conflict*, Vol. 52(4), pp. 537– 552.

Rustad, S. C. A., Buhaug, H., Falch, A. & Gates, S. (2011). 'All Conflict is Local Modeling Sub-National Variation in Civil Conflict Risk'. *Conflict Management and Peace Science,* Vol. 28 (1), pp. 15-40.

Sambanis, N. (2001). 'Do Ethnic and Nonethnic Civil Wars Have the Same Causes?: A Theoretical and Empirical Inquiry (Part 1)'. *The Journal of Conflict Resolution*, Vol. 45, No. 3, pp. 259-282.

Sambanis, N. (2004). 'What Is Civil War? Conceptual and Empirical Complexities of an Operational Definition'. *Journal of Conflict Resolution*, Vol. 48, No. 6, pp. 814–858.

Sambanis, N. (2005). 'Conclusion: Using case studies to refine and expand the theory of civil war'. In: Collier, P. & Sambanis, N. (eds) *Understanding Civil War: Evidence and Analysis*. Washington, DC: World Bank, pp. 303–334.

Sambanis, N., & Shayo, M. (2013). Social identification and ethnic conflict. *The American Political Science Review*, Vol. 107(2), pp. 294–325.

Saucier, G., Akers, L.G., Shen-Miller, G. (2009). 'Patterns of thinking in militant extremism'. *Perspectives on Psychological Science,* Vol. 4(3), pp. 256–271.

Schneider, G. & Wiesehomeier, N. (2008). 'Rules that matter: Political institutions and the diversity–conflict nexus'. *Journal of Peace Research*, Vol. 45(2), pp. 183–203.

Shaykhutdinov. R. & Bragg, B. (2011). 'Do Grievances Matter in Ethnic Conflict? An Experimental Approach'. *Analyses of Social Issues and Public Policy*, Vol, 11(1), pp 141-153.

Sirin, C.V. (2011). 'Scarcity-Induced Domestic Conflict: Examining the Interactive Effects of Environmental Scarcity and 'Ethnic' Population Pressures'. *Civil Wars*, Vol. 13:2, pp. 122-140, Available at: DOI: 10.1080/13698249.2011.576141

Smirnova, A. & Iliev, R. (2017). 'Political and Linguistic Identities in an Ethnic Conflict'. *Journal of Language and Social Psychology* 2017, Vol. 36(2), pp. 211– 225.

Snyder, J. L. (2000). *From Voting to Violence: Democratization and Nationalist Conflict*. New York: Norton.

Snyder, H. (2019). Literature review as a research methodology: An overview and guidelines. *Journal of Business Research*, Vol. 104, November 2019, pp. 333-339.

Spain, D. (1993). 'Been-heres versus come-heres negotiating conflicting community identities'. *Journal of the American Planning Association*, Vol. 59(2), pp. 156-171.

Stewart, F. (2002). 'Horizontal inequalities: A neglected dimension of development'. *QEH* Working Paper Number 81. Queen Elizabeth House, University of Oxford.

Stewart, F. (2008). *Horizontal Inequalities and Conflict*. New York: Palgrave Macmillan.

Stroschein, S. (2017). 'Ethnic Conflict: Looking Inside Groups'. *Ethnopolitics*, Vol. 16:1, pp. 74-81, Available at: DOI: 10.1080/17449057.2016.1235830

Tajfel, H. &Turner, J.C. (1979). 'An integrative theory of intergroup conflict'. In: Austin WG, Worchel S (eds) *The social psychology of intergroup relations*. Brooks/Cole, Monterey, pp. 33-47.

Tajfel, H. & Turner, J.C. (1986). 'The Social Identity Theory of Intergroup Behavior.' In: Worchel, S. & Austin, W.G., (eds.)., *Psychology of Intergroup Relation*, Hall Publishers, Chicago, pp. 7-24.

Toft, M. D. (2002). 'Indivisible territory, geographic concentration, and ethnic war'. *Security Studies,* Vol. 12(2), pp. 82-119.

Toft, M. D. (2003). *The geography of ethnic violence: Identity, interests, and the indivisibility of territory.* Princeton, NJ: Princeton University Press.

Toft, M. D. (2007). 'Getting religion? The puzzling case of Islam and civil war'. *International Security*, Vol. 31(4), pp. 97-131.

Toft, M. D. (2017). 'The Field of Ethnic Conflict Studies: An Interplay of Theory with Reality'. *Ethnopolitics*, Vol. 16:1, pp. 5-11, Available at: DOI: 10.1080/17449057.2016.1235350

Vanhanen, T. (1999). 'Domestic Ethnic Conflict and Ethnic Nepotism: A Comparative Analysis'. *Journal of Peace Research*, vol 36, no.1, 1999, pp. 55-73.

Vanhanen, T. (2012). 'Ethnic Conflict and Violence in Heterogeneous Societies.' *The Journal of Social, Political and Economic Studies*, Vol. 37(1), pp 38-66.

Varshney, A. (2002). *Ethnic Conflict and Civic Life: Hindus and Muslims in India*. New Haven: Yale University Press.

Wegenast, T. C. & Basedau, M. (2014). 'Ethnic fractionalization, natural resources and armed conflict'. *Conflict Management and Peace Science*, 2014, Vol. 31(4), pp. 432-457.

Walker, I., & Pettigrew, T. F. (1984). 'Relative deprivation theory: An overview and conceptual critique'. *British Journal of Social Psychology*, Vol. 23(4), pp. 301-310.

Watts, S., Kavanagh, J., Frederick, B., Norlen, T. C., O'Mahony, A., Voorhies, P., Szayna, T. S. (2017). 'Understanding Conflict Trends: A Review of the Social Science Literature on the Causes of Conflict.' Research Report. Published by the *RAND Corporation*, Santa Monica, California.

Weidmann, N. B. (2009). 'Geography as motivation and opportunity: Group concentration and ethnic conflict'. *Journal of Conflict Resolution,* Vol. 53(4), pp. 526-543.

Weidmann, N. B. (2011). 'Violence "from above" or "from below?" The Role of Ethnicity in Bosnia's Civil War'. *Journal of Politics,* Vol. 73 (4), pp. 1-13.

Wellman, J.K. & Tokuno, K. (2004). 'Is religious violence inevitable?' *Journal for the Scientific Study of Religion,* Vol. 43(3), pp. 291-296.

Wimmer, A., Cederman, L-E. & Min, B. (2009). 'Ethnic Politics and Armed Conflict: A Configurational Analysis of a New Global Data Set'. *American Sociological Review,* Vol. 74 (2), pp. 316-37.

Wimmer, A. (2013). *Ethnic Boundary Making: Institutions, Power, Networks*. Oxford: Oxford University Press.

THE STRATEGIC INTERPLAY BETWEEN RESILIENCE AND COVID-19 PANDEMIC: APPROACHES, ASSETS, AND AMBITIONS

George Mihael Manea, PhD
Romanian Ministry of Internal Affairs
Civil servant in the field of resilience building and international cooperation
University of Bucharest
Associate professor

Keywords: resilience, Covid-19, crisis, cooperation, international organisations

ABSTRACT

As the world enters a new decade, the outbreak of Covid-19 suddenly occurred and spread rapidly from certain regions to the entire world. It hence becomes a public health emergency threatening the health and safety of mankind. Over the past months, many studies and analyses have been published concerning the political, economic, and social effects of Covid-19. This article provides a review of the concept of resilience and explores the puzzle of resilience within international organisations, such as EU, NATO, and UN, in the context of the pandemic, along with a case study on the Romanian practical experience in trying to build and increase societal resilience during the first wave of Covid-19.

In the unpredictable real-world environment, international organisations try to redefine their strategies and goals. The aim of this article is to answer at two important research questions, such as '*How can international organisations develop a multi-layered and integrated toolbox in building resilient societies?*' and '*To what extent can member states use this toolbox to increase their strengths and overcome weaknesses in crisis management?*'. The article also bears relevance to the area of internal security, and the topic raises the issue of adaptability in concepts and actions, making the transition from an international organisations perspective to nation states in the context of resilience and Covid-19 response.

In terms of methodology, qualitative research methods will be used for the further development of this article, including first-hand sources, such as books, academic papers and working documents, but also official websites and interviews. At the same time, Analysis of Alternatives (AoA) techniques will be part of the case study to highlight decisions and initiatives that have been taken in dealing with Covid-19 challenges.

INTRODUCTION

Motto: 'By failing to prepare, you are preparing to fail'
(Benjamin Franklin)

The whole world is in a critical moment, in a diversity of crises, from sanitary to economic, from conspiracy to fake news. In the fight against the pandemic, international organisations have made full use of their institutional advantage of concentrating resources to accomplish large undertakings. Solidarity and cooperation are important among the international community to overcome the new Coronavirus (SARS-CoV-2); however, there are various obstacles related to language, culture and medical situation in different countries that require particular attention and assistance.

The global Covid-19 pandemic has affected almost all areas of life. Governments worldwide struggle with the social and economic consequences of the crisis. During the early phases of the pandemic, it became evident that certain sectors have been particularly challenged by Covid-19. Starting from issues, such as providing personal protective equipment to the healthcare sector or increasing capacities in intensive care units, more and more challenges emerged during the current pandemic context.

While the origins of the virus are not known and many experts are intensifying their efforts to identify adequate measures for fighting against Covid-19, most of the countries are confronted not only with a public health issue but also a societal and security crisis. Critical infrastructure operators have activated their crisis management plans in various sectors, such as energy, telecommunications, transport and logistics, while the work of healthcare and civil protection authorities has increased considerably within this period of time.

Covid-19 has served to remind us about the importance of resilience, acting as an eye-opener to the whole spectrum of crisis management structures and high impact low probability (HILP) events. From this

point of view, civil preparedness has become even more important, with a focus on healthcare system and continuity supply as part of the continuity process (i.e. keep operational in terms of business continuity, make operational plans for medium and long term, build stockpiles through procurement, donations and trust funds).

Governments and national authorities must take responsibility for disaster risk reduction in all areas to anticipate vulnerabilities and implement business continuity plans. Disaster risk management is primarily aimed at protecting people and properties, but also their health, livelihoods, and vital resources of the economy, environment and cultural heritage. The fight against large-scale disasters can only be ensured through effective collaboration, joint policies and actions to resolve crises. Based on this approach, it is necessary to build partnership frameworks to become more resilient and agile as well as to react promptly to the impact of Covid-19, as it is already known that 'viruses, bacteria, and various kinds of plants and animals have never respected national borders' (Pirages and Runci, 2000, p. 178).

The concept of resilience involves a multitude of possible answers adapted to the reality and circumstances. It is an interdisciplinary and multilayered concept that can be applied at all levels: individual, regional, national or international. As resilience goes hand in hand with vulnerability and fragility, it is important to emphasise that planning and immediate response in crisis management are key tools. Building a more resilient society requires strengthening shock absorption mechanisms and increasing adaptability. However, 'addressing the Covid-19 pandemic and its effects on society requires more than the actions of healthcare and medical professionals alone. It calls for engagement of citizens, governments at all levels, and a diverse array of organisations and individuals involved in policymaking processes and policy implementation' (Weible et al., 2020, p. 3).

The role of international organisations must be to help each other, to collaborate for integrative management and governance, allowing learning and flexibility in building adaptability at all levels of society. The international mechanisms of assistance created by NATO, the EU, and the UN increase the level of resilience of their member states, as well as the ability of citizens to react and adapt to the measures needed to ensure continuity

and recovery from a disaster and/or a crisis. International organisations have developed strategies, programmes, and toolbox packages to prevent and increase the level of resilience. However, now they must adjust them to become parts of a more integrated approach.

Each international organisation has a different approach to tackling Covid-19: on the one hand, NATO acts as an integrator, oriented towards an all-hazards approach, highlighting the link between *security* and resilience; on the other hand, the EU is a multi-nodal provider, oriented towards a 360-degrees system approach, having at core the link between *society* and resilience; while the UN serves as a facilitator, oriented towards people's resilience and emphasising the link between *development* and resilience. Thus, in order to make this multilateralist scheme functional, 'there must be consensus on what it is supposed to do, and can realistically achieve' (Trenin et al., 2020, p. 7) through solidarity, international cooperation, transparent approach, considering multiple types of impact and investing more in data collection and epidemic forecast.

Hence, this article will try to bring an answer to the research questions framed as following: '*How can international organisations develop a multi-layered and integrated toolbox in building resilient societies?*' and '*To what extent can member states use this toolbox to increase their strengths and overcome weaknesses in crisis management?*'. In terms of structure, the article consists of two parts: the first part will analyse the involvement of international organisations (i.e. NATO, the EU, the UN) in building resilient societies and tackling Covid-19, while the second part presents a case study of the Romanian strategic response to the pandemic in the context of cooperation with international organisations, civil society, and the private sector. In terms of research methodology, I will be using qualitative data with a focus on primary sources, such as books, academic papers, working documents, official websites and interviews, but also the Analysis of Alternatives (AoA) technique for the case study.

This article has been written during the pandemic period, far from being over and before reaching its second peak. Some aspects related to the topic of this article thus remain underanalysed and deserve more attention in the aftermath of the Covid-19 pandemic. However, a preliminary overview on the measures, coordination processes, and toolbox packages (mechanisms, instruments, and platforms) offered by international

organisations to increase societal resilience during this sanitary crises, backed-up by observations and lessons learned collected at the national level, can definitely help to mitigate the negative effects and consequences of the pandemic.

1. COOPERATION AND RESILIENCE OF INTERNATIONAL ORGANISATIONS IN THE CONTEXT OF COVID-19

1.1 NATO'S APPROACH – THE LINK BETWEEN SECURITY AND RESILIENCE

Resilience is seen by the Alliance as 'the society's ability to resist and recover easily and quickly from such shocks and combines both civil preparedness and military capacity. Robust resilience through civil preparedness in Allied countries is essential to NATO's collective security and defence' (NATO website). Moreover, resilience is a national responsibility under Article 3 of the NATO Treaty: 'in order more effectively to achieve the objectives of this Treaty, the Parties, separately and jointly, by means of continuous and effective self-help and mutual aid, will maintain and develop their individual and collective capacity to resist armed attack' (The North Atlantic Treaty, 1949).

In this context, resilience represents not only the Allies' development capacity to ensure collective and individual security, but also their capacity to deal with crisis situations: affected critical infrastructures (transport corridors, communication networks, energy supply), natural disasters, limited access to vital resources, etc. The roots of this concept of resilience can be found in NATO's New Strategic Concept: Active Engagement, Modern Defence adopted by the NATO Summit in Lisbon back in 2010, discussed in some detail in paragraph 13:

> All countries are increasingly reliant on the vital communication, transport and transit routes on which international trade, energy security and prosperity depend. They require greater international efforts to ensure their resilience against attack or disruption. Some NATO countries will become more dependent on foreign energy suppliers and in some cases, on foreign energy supply and distribution networks for their energy needs. As a larger share of world consumption is transported across the globe, energy supplies are increasingly exposed to disruption (NATO, 2010, p. 6).

The concept of resilience extended to civil preparedness was subsequently highlighted at the 2016 NATO Summit in Warsaw in relation to the adoption of the Final Communiqué:

- we have taken a range of steps to reinforce our collective defence, enhance our capabilities, and strengthen our resilience, and

- civil preparedness is a central pillar of Allies' resilience and a critical enabler for Alliance collective defence. While this remains a national responsibility, NATO can support Allies in assessing and, upon request, enhancing their civil preparedness. We will improve civil preparedness by achieving the NATO Baseline Requirements for National Resilience, which focus on continuity of government, continuity of essential services, security of critical civilian infrastructure, and support to military forces with civilian means (Warsaw Summit Communiqué, 2016).

The commitment to enhance resilience is based on 'the recognition that the strategic environment has changed, and that the resilience of civil structures, resources and services is the first line of defence for today's modern societies' (Roepke and Thankey, 2019). At the NATO level, there are three essential functions that a state must perform in all circumstances from the civilian perspective: (i) continuity of governance, (ii) continuity of provision of basic services to the population, (iii) civilian support for military operations. However, baseline requirements for resilience should be seen as a process of implementation at the political and societal level, working in close cooperation with international partners and taking into account a full spectrum of operations, setting the level of ambition, including a variety of means and areas of planning.

The *whole of government approach* is crucial but might not be enough to effectively deal with crises. Implementing a *whole of society approach* will bring benefits on the civil-military cooperation, will enable crisis management efforts, and allow nations to have a cross-sectoral, holistic view of resilience planning and civil preparedness at all times. In essence, the transition from whole of government approach towards whole of society approach reflects the complexity and interdependencies of modern society, and builds resilience at all levels (i.e. civil and military, public and private).

Covid-19 has led to a renewed discussion on the level of ambition and direction on resilience framework, including civil preparedness. NATO remained concerned about the evolution of the new Coronavirus worldwide and during the NATO Defence Ministerial Meeting, it was decided 'to update NATO's guidelines for national resilience to take greater account of cyber threats, the security of supply chains, and consequences of foreign ownership and control' (NATO, 2020a).

The first step was taken by NATO's Civil Emergency Planning Committee (CEPC), which aims at the protection of the civil population and supports NATO's strategic planning for the use of civil resources in support of the Alliance's objectives in a systematic and effective way. CEPC leads and coordinates the civil emergency planning activities to guarantee civil support for NATO's military operations or support for national authorities in civil emergencies. Four specialised groups operate in the context of the CEPC: the Civil Protection Group (CPG), the Transport Group (TG), the Joint Health, Agriculture and Food Group (JHAFG), and the Industrial Resources and Communications Services Group (IRCSG). These groups connect government representatives, industry experts and military representatives to coordinate and develop the emergency preparedness arrangements in these areas (NATO website). This allowed NATO to be directly involved in mitigating the effects of Covid-19, both for its Allies and its partners, by building new modular field hospitals, sending military professionals to help the civilian hospitals, providing new treatments beds, contributing with airlifting capabilities or sending interdisciplinary teams of experts.

Moreover, NATO's efforts to enhance resilience and fight against Covid-19 were also facilitated by a multi-year project launched within the framework of NATO's Science for Peace and Security Programme (SPS). The main partners of the project, Italian National Health Insitute, Tor Vergata University Hospital, and University Hospital of Basel University, have defined their main objective as 'enhanc[ing] the speed and efficiency of Covid-19 diagnosis through a multidisciplinary approach, by bringing together experts in the field of immunology, virology, and molecular biology' (NATO, 2020b). By working together, 'scientific and technical experts can help specify the severity of Covid-19 in a population, project its trajectories over time, and estimate the likely effects of different policy responses, from mitigation to suppression' (Weible, 2020, p. 8).

NATO is adapting to new realities and needs to tackle the effects of the pandemic. Thus, as an integrator, NATO has concentrated on logistics and contingency planning, being able to meet a multitude of risks (all-hazards approach) through different levels of cooperation:

a) *Civil-military cooperation*: the military side has been involved in providing assets and capabilities, medical and non-medical support, transport corridors, access to resources in real time, robust security of supply arrangements and logistics as a key component of the response efforts;

b) *Cross-sectoral cooperation*: dedicated and scalable planning (contingency planning), especially in sectors, such as energy, transportation, communication networks, food and water. As all of them represent civilian assets in most cases, it is important to protect them and to enhance resilience, as they might be highly vulnerable to internal disruptions and/or external attacks: 'a high level of interconnectedness [supply, trade and delivery of goods and services] is more efficient and allows for economies of scale. But greater interdependencies also increase the risk of cascading effects in the event of a disruption' (Roepke and Thankey, 2019);

c) *International cooperation*: partnership, coordination and harmonisation of similar measures are paramount in order to save lives. The EU is a critical partner in building resilience, being able to overcome HILP consequences through resilient societies. Working together, both NATO and EU can engage with citizens of their member states: 'resilient societies also have a greater propensity to bounce back after crises: they tend to recover more rapidly and are able to return to pre-crisis functional levels with greater ease than less resilient societies. This makes continuity of government and essential services to the population more durable' (Roepke and Thankey, 2019).

In conclusion, NATO's resilience derives from the resilience of each ally. Therefore, steps should be taken by each member state to increase its societal resilience at the national level. Navigating the same waters during the Covid-19 crisis means that everyone should look at the same map to understand the real challenges and work together in crisis management. Thus, civil preparedness and the seven baseline requirements have

energized NATO's approach to resilience in the context of the pandemic, being complementary with the approach of other international organisations and an added value for both its allies and partners.

1.2 THE EU'S MECHANISMS FOR THE CONSOLIDATION OF SOCIETY AND RESILIENCE

At the EU level, resilience is defined as 'the ability of an individual, a household, a community, a country or a region to withstand, to adapt, and to quickly recover from stresses and shocks' (European Commission, 2012, p. 5). As the EU highlights the link between society and resilience, building societal resilience and enhancing additional civil protection instruments and tools represent a step forward in crisis management: 'societal resilience needs to be tackled with a 360-degrees system approach, which help to look at complexities and interconnections' (Giovannini et al., 2020, p. 3).

For the EU, building societal resilience remains the primary target to be achieved: '[B]e able to face shocks and persistent structural changes in such a way that societal well-being is preserved, leaving no-one behind (intra-generational equity) and without compromising the heritage for future generations (inter-generational equity and sustainability)' (Giovannini et al., 2020, p. 5). Hence, trust between citizens and governments plays a key role and people should know that they can rely on state authorities in times of crisis, and simultaneously authorities can rely on citizens. This will lead to a resilient society, aware of its role in challenging situations and willing to work hand in hand with state authorities.

In terms of instruments and tools, the EU is 'mobilising all resources available to help Member States coordinate their national responses, and this includes providing objective information about the spread of the virus, the effective efforts to contain it and measures taken to repair the economic and social damage brought by the pandemic' (European Union, 2020a). In order to further reinforce the collective ability of the EU and its members states to respond to disasters, address recurring and emerging capacity gaps, and enhance its administration procedures, new legislation to strengthen the European policy on disaster management

was introduced in March 2019. In accordance with the amendment, the core elements of the Union Civil Protection Mechanism (UCPM)[1] are now as follows: the Emergency Response Coordination Centre (ERCC), the Common Emergency Communication and Information System (CECIS), the European Civil Protection Pool, the rescEU reserve and the Emergency Support Instrument (ESI) – (Official Journal of the European Union, 2019, L 77 I).

One of the new measures is the rescEU reserve, designed to strengthen the existing capacities, to respond to overwhelming situations as a last resort and to ensure an effective response to severe trans-boundary disasters. It includes a fleet of fire-fighting planes and helicopters, medical evacuation planes, as well as a stockpile of medical equipment and field hospitals that can respond to health emergencies, and chemical, biological, radiological, and nuclear incidents (European Commission, 2019). Taking into account the evolution of the pandemic situation in the EU territory, the European Commission was interested in creating a strategic medical stockpile through rescEU and UCPM, being hosted at the EU level, in its first phase, by Romania and Germany. The rescEU includes 'medical equipment, such as ventilators, personal protective equipment, vaccines and therapeutics and laboratory supplies' (European Commission, 2019) and has been extended to six states adding Denmark, Greece, Hungary and Sweden.

Another new measure was introduced with the EU decision to make a step forward in protecting its members states by offering a new instrument in tackling the effects of the pandemic as it is the case of the Emergency Support Instrument launched in 2020. It will include vaccine supplies once the production of vaccines starts at the EU level; treatments with authorised medicines at the EU level to treat Covid-19 (e.g. Remdesivir); transport of essential goods, medical teams and patients to provide medical assistance; essential health related products with a particular focus on the personal protective equipment and training of healthcare professionals in intensive care skills (European Union, 2020b).

[1] The UCPM was established in 2001. In the almost twenty years since its establishment, the Mechanism has been activated for over 300 emergencies, including the Ebola outbreak (2014), the earthquake in Nepal (2015), forest fires in Europe, tropical cyclones Irma and Maria in the Caribbean (2017), floods in the western Balkans (2014), and the migration and refugee crisis (2015).

The Covid-19 pandemic has shown that each EU member state can be affected and that the member states have responded differently based on domestic situation. Uncoordinated responses could lead to inadvertent and undesirable consequences. The variety of responses, especially at the beginning of the crisis, led to inadvertent distortions in the functioning of the single market (e.g. the free flow of goods, in particular the transport of essential goods and services, such as medical equipment, medicines and food supply was disrupted). In addition, many EU citizens staying abroad were unable to return home and in several instances frontier workers experienced severe delays at internal borders.

These unpredictable consequences of the Covid-19 pandemic have further shown the need for more and better EU preparedness for future large-scale emergencies, including HILP. Taking into consideration the proven limitations of the current framework, the interconnected nature of societies confronting the same emergency, and the resulting difficulty in helping each other, it becomes clear that enhanced action is needed both at the Union level as well as between member states.

From the examples presented, it is clear that the EU and its member states tried to ensure their own readiness and resilience to crises to their full extent. However, efficient resilience systems are based on absorptive capacity, adaptive capacity and transformation, but also need 'behavioral shifts and institutional reforms (including changing priorities, challenge beliefs and stereotypes)' (Giovannini et al., 2020, p. 6). Moreover, a long-term resilience approach needs a coherent strategy based on strengthening the level of education and building a culture of preparedness, or culture of safety, especially designed for disasters and emergencies. Increased communication, information and dissemination, together with a '*think of the unthinkable mindset*' can lead to behavioural change and community resilience (Office Journal of the European Union, 2013, C468/124).

This pandemic tested the resilience of societies, showing at the same time a glass half full (development of technological assets and infrastructure, exchange and interoperability of medical personnel, high speed trains used to move infected patients, field modular hospitals and laboratories built, etc.) and a glass half empty (lack of preventive measures, unprepared societies and states to deal with the pandemic consequences, the stockpiling issue, the changing prices, cancelled signing agreements,

fake products, etc.). This way, a mix of targeted measures – as shown in the table below – could increase the level of resilience and highlight the progress made and the things left to be done.

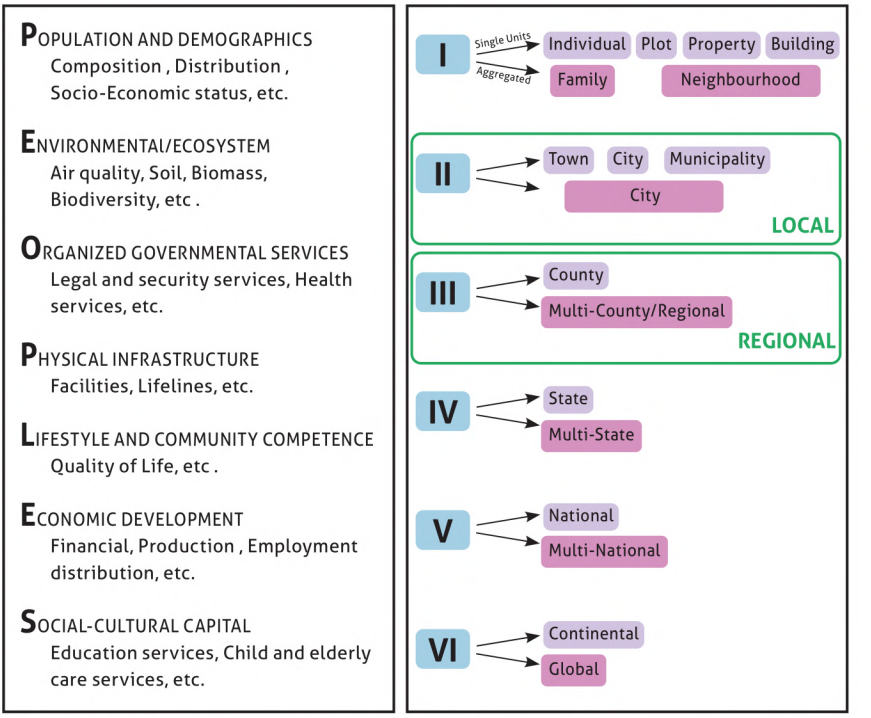
Policies	Aim
Preventive measures	Aim to reduce the incidence and size of shocks (e.g. red zones to limit contagion).
Preparation measures	Aim to prepare for handling them successfully (e.g. reinforcing the health capacity with extra resources to face the emergency, strengthening medical research efforts to find a vaccine).
Protection measures	Required to mitigate the impact and support the absorptive capacity (like state support to economy, SMEs or the most hit sector like tourism, or benefits for families which are forced to telework).
Promotion measures	Serve to increase the adaptive capacity or flexibility.
Transformation measures	Restart and redesign production chains, re-evaluate healthcare and working practices.

(Giovannini *et al.*, 2020, p.8).

In conclusion, strengthening resilience at the EU level requires tailor-made approaches and identification of mechanisms to continuously contribute to sustainable results (as it was the case with rescEU and ESI). It is clear that 'the current crisis has shown at least one important lesson for Europe: solidarity is not a given and it takes will to fight for what one stands for. The level of cooperation between EU Member States was indeed uncoordinated and far too limited at the beginning of the crisis though followed by a range of actions in medical assistance and recovery funds [however] Europe has a unique role to play in seeking to foster multilateral and regional cooperation' (Trenin et al., 2020, p. 11). Thus, resilience requires risk-informed programming, but also a comprehensive analysis of strengths, vulnerabilities and pressures (European Commission, 2017, p. 24) taking into account the complex interdependencies among all actors involved.

1.3 UNITED NATIONS THE COMMON GROUND FOR DEVELOPMENT AND RESILIENCE

The UN is a catalyser of sustainable development and resilience, defining the resilience process as 'the ability of any urban system to maintain continuity through all shocks and stresses while positively adapting and transforming towards sustainability. Therefore, a resilient city is one that assesses, plans and acts to prepare for and respond to all hazards, either sudden or slow-onset, expected or unexpected. By doing so, cities are better able to protect and enhance people's lives, secure development gains, foster and investible environment and drive positive change' (United Nations Habitat website).



Description of the PEOPLES Resilience Framework and its associated geographical scale (Renschler, 2013, p.3)

While NATO has seven baseline requirements for resilience and the EU has developed two instruments for multi-layer crisis management (i.e. rescEU and ESI), the UN has proposed the PEOPLES Resilience Framework as a tool for building resilience, with the primary objective of creating frameworks for partnerships and improve pre- and post-disaster cooperation and communication for better crisis management. At the UN level, the approach is similar to both NATO and the EU, with a focus on population and demographics, environment and ecosystems, organised governmental services, physical infrastructure, lifestyle and community competence, economic development and social-cultural capital, having at core the citizens and their society.

From the UN's perspective, building a resilient community is directly related to their level of preparedness and ability to face shocks and deal with multiple challenges, such as education, health, demographic imbalances, climate change, migration, peace and security.

The United Nations, through the UN Office for Disaster Risk Reduction (UNDRR), has its own paradigm ('living with risk') and is geared towards reducing socio-economic and humanitarian disasters through concrete measures. The UN presents an ideology, a worldview through the use of a certain language, namely to build a better and more secure world. Based on the UN's Sustainable Development Goals (SDG), resilience is not an empty ship but a sense of direction in international negotiations in order to reach a resilient society (Wiig and Fahlbruch, 2019).

The UN SDG can be seen from an integrated and interconnected perspective as a path to achieving resilience at community level. Thus, the Covid-19 pandemic reveals 'a rare opportunity to redesign global and national systems for managing deadly risks, using science-based evidence and information communication technology, to identify, track, search, and share timely, valid data among nations, triggering innovation and collective action to build a resilient international community. Bold redesign of existing international organizations – the WHO, OCHA, and UNDRR – that monitor and compare the status of global risk would reinforce cognition in facilitating effective crisis response across the globe by partnering with nations to work with their local communities' (Comfort et al., 2020, p.621).

In the context of the current article, the goal no. 11 on sustainable cities and communities seems to be the most relevant for analysis as 'cities are on the front line of coping with the pandemic and its lasting impacts [...] Covid-19 is threatening cities and communities, endangering not only public health, but also the economy and the fabric of society' (United Nations website, 2020). Having already witnessed similar events at a lower scale, such as SARS-COV in Guangdong, China (2002), MERS-COV in Middle East (2012), Ebola outbreak in West Africa (2014–2016), Zika outbreak in Brazil (2015–2016), and now Covid-19 (SARS-COV-2) all over the world, it is important to understand the dynamics related to pandemic and its multiple dimensions of impact, as well as to define clear roles and responsibilities, both for international organisations and member states.

Community-driven solutions, including top-down and bottom-up approaches, can lead to preventive and preparation measures that can help in crisis management situations. National legislation is a key factor in building societal resilience, as it provides legitimacy and support for the population's trust in local and national authorities. Moreover, 'awareness of the threat that infectious disease outbreaks could pose to their citizens' health and to their countries' economic and political stability encouraged western governments to develop responses in national security terms' (Davies, 2008, p. 298).

In conclusion, even if the UN was supposed to have the necessary framework to deal with the global pandemic through the World Health Organisation (WHO), it ended up with weak coordinated support and lack of clear communication on some preventive measures for its member states. As a result, health challenges affect 'the bilateral and regional political relationships between developed and developing countries, and influence strategies for United Nations reform. Although health has long been a foreign policy concern, such prominence is historically unprecedented' (Fidler and Drager 2006, p. 687).

In this regard, it is of utmost importance that the UN starts to cooperate closely on resilience with the other international organisations, such as NATO and the EU. This is highly recommended to strengthen its work on civil protection and resilience post Covid-19, but also to gain in terms of regulatory function, dialogue and cooperation.

1.4 COMPARATIVE PERSPECTIVE ON NATO, EU AND UN APPROACHES IN BUILDING RESILIENT SOCIETIES

Resilience is still a new concept, there are numerous gaps between theory and practice, the desk and the field, negotiations and talks and real challenges and impact on the ground. Despite Covid-19, the vulnerabilities found in many communities around the globe require a new approach not only from international organisations but also from states themselves. However, this has to be done in full cooperation and partnership, not in competition or isolation. Globally, 'Covid-19 has laid bare the limits of a governance architecture that merely monitors and suggests, rather than enforces [...] pointing to the need for more global coordination and cooperation' (Trenin et al., 2020, p. 8).

After a short overview of the toolbox packages provided by the international organisations, such as NATO, the EU, and the UN for building resilient societies and coping with the Covid-19 pandemic, there is still a lot of work to be done to prepare communities and make societies resilient. In recent years, both NATO and the EU have increasingly assumed responsibility for and leadership of the protection of civilians, and are becoming key players as crisis managers. Even though NATO and the EU have declared that the member state where a crisis occurs bears the brunt of the responsibility for managing its immediate effects, there is a consensus in both organisations that disasters, whether natural or man-made, can overwhelm national resources in civil protection and necessitate outside assistance to manage the emergency (Boin and Lodge, 2016, p. 293).

Even if member states bear the primary responsibility for crisis management, the current crisis has raised questions regarding the organisation of a coordinated response including multi-layer resilience building and the development of an adequate toolbox for crisis management. The role played by national authorities and coordination at the level of international organisations are paramount to dealing with Covid-19. It is important to emphasise that solidarity and unity are not only goals in themselves but also a key to overcoming the challenges created by the pandemic. Moreover, it also becomes a duty of governments to prepare citizens to be resilient and self-sufficient for up to 72 hours.

As nobody can act in isolation, the EU needs a strong partnership with other international organisations, such NATO and the UN. On the one hand, the dual membership of most European countries in both NATO and the EU emphasises the identity, values, and interests on which the coherence and cohesion of the two international organisations are based. On the other hand, in its position as a global actor, the EU has 'a particular responsibility to help frame a global response through multilateralism and a rules-based international order, with its partners in the UN [...] re-establishing trade flows and supply routes is of the utmost importance. At the same time, the EU must provide assistance to countries in need' (The Presidents of the Council and the Commission, 2020, p. 4).

The current crisis highlights 'the world's tremendous need for an international system that can actually exercise collective problem-solving authority' (Trenin et al., 2020, p. 4). From this point of view, Covid-19 represents an unfortunate example. The lack of global solidarity and leadership during the Covid-19 pandemic compared with the Ebola outbreak (2014–2016), which saw cooperation between all actors, is calling into question the role of multilateralism. So far, what we have witnessed is a fragmented and polarised global scene with aspects of nationalism and isolationism. The first reactions to the pandemic cast international cooperation in a negative light. Initially, states resorted to unilateral measures, without cooperating with major partners, and international organisations had limited or even delayed and outdated involvement for various reasons, as seen in public space. At the same time, the Covid-19 brought on an unprecedented global crisis in the era of globalisation which should make international organisations and governments develop resilience tools applicable on a broader and interconnected scale.

Last but not least, medical diplomacy is emerging as a new feature on the global stage. The diplomacy of masks or China's Belt and Road Initiative as tools for coordination and multilateral action under Chinese leadership in the field of health have shown lack of coordination and weaknesses of the Western states, together with massive disinformation campaigns oriented towards their societies: 'mass donation of masks and supplies to ailing hospitals and local charities are pivotal in rehabilitating China's historically maligned and recently ignominious image in particular areas [as well as] emphasis upon establishing long-term dependence relations and patronage networks' (Wong, 2020). The reform of the multilateral

system must include the global health architecture and lessons learned from the pandemic, respectively the launch of a preparedness initiative as part of the Sustainable Development Goals.

Having looked at various approaches, assets, and ambitions of the international organisations in the first part of the article, the second part will analyse a concrete example of how some of these resilience tools have been applied in the Romanian experience in dealing with pandemic. The case study will highlight the Romanian strengths and weaknesses in tackling the Covid-19 pandemic, first in terms of cooperation with international organisations through their capabilities and mechanisms (including strategies for population's behaviour change on the longer run), and second with civil society and private sector in taking adequate measures at the national level to build societal resilience.

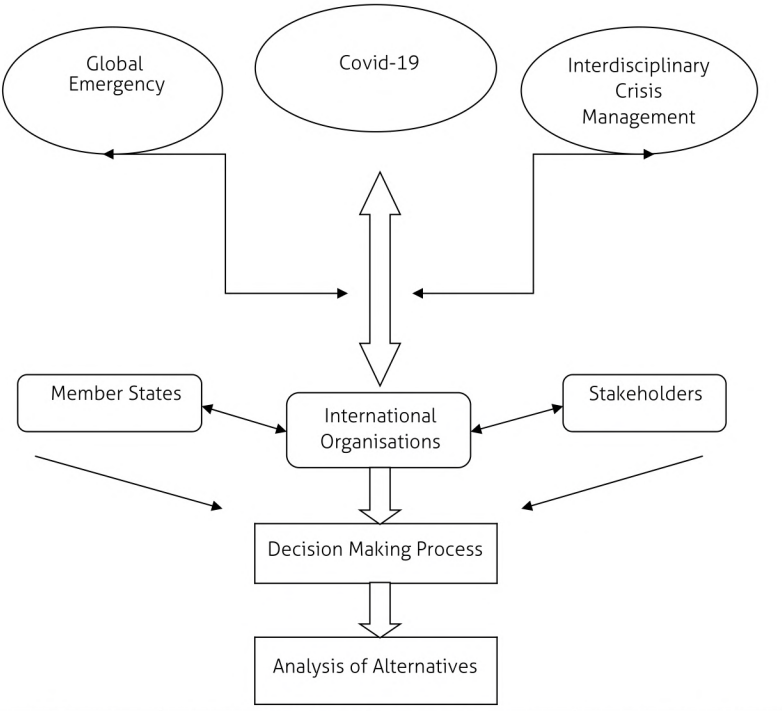
2. CASE STUDY: ROMANIAN STRATEGIC RESPONSE TO COVID-19

This case study will not go into the details of all the aspects related to the Romanian strategic response to Covid-19, but it will discuss cooperation with international organisations (i.e. on airlifting capabilities, mechanisms for civil protection, initiatives for population behaviour change), and cooperation with the civil society and private sector (i.e. on technological initiatives that have been developed to help communities and reach societal resilience).

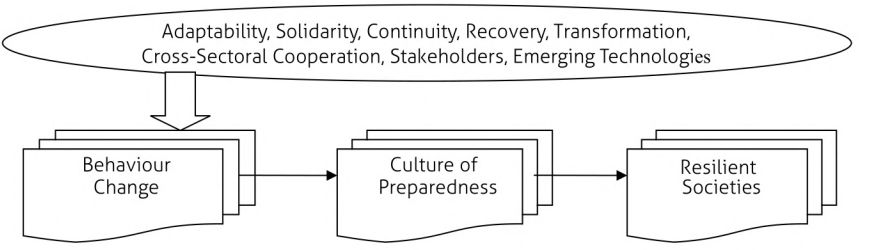
The current pandemic crisis has renewed 'attention to the importance of, and how little we know about, learning under stress and urgency in the middle of a crisis' (Boin *et al.*, 2005, p. 15). Considering the fact that parallel and micro-management represented a challenge at the level of decision-making process, Analysis of Alternatives (AoA) can be used for demonstrating alternatives techniques that can provide added value within coordination and command at the national level. AoA represents an important analytical practice 'to reduces risk and expands opportunities for innovative solutions, creating space for more timely decisions [...] diagnosing problems, understanding complicated situations, challenging plans' (NATO, 2017) based to the scheme below:

Following my direct involvement in cooperation and management activities within the Romanian Department for Emergency Situations related to Covid-19 pandemic, I will sometimes make reference to my practical experience to highlight the Romanian government's cooperation with international organisations, civil society and private sector while still trying to maintain an unbiased perspective.

Top-Down Approach in Decision-Making



Structuring Techniques	Creative Techniques	Diagnostic Techniques	Challenge Techniques
Mind Mapping	Brainstorming	SWOT / PMI	Devil's Advocacy
Concept Mapping	Brainwriting	Outside-In Thinking	Pre-Mortem Analysis
Rich Pictures	Six Thinking Hats	Five Whys	What-If Analysis



Plusses	Minuses	Interesting
Cooperation with international organisations	Lack of stocks / reserves of specialised protective equipment	Innovation through technological solutions
Civil-military cooperation	Lack of preparedness culture	Hybrid challenges and disinformation campaigns
Cooperation with civil society and private sector	Lack of clear and coherent emergency legislation	Green line for psychological and moral support
Integrated command and coordination centre for decision-making	Excessive use of Covid-19 as a playground for political reasons	Telework measures
Interconnectivity of the seven baseline requirements of resilience	Huge return of diaspora	ERCC and EADRCC
Strategic Communication Group	Vulnerability of communities in the light of Covid-19	rescEU, ESI, RVM

Example of AoA Diagnostic Technique: Romanian PMI for decision-making

2.1 ROMANIA'S COOPERATION WITH INTERNATIONAL ORGANISATIONS

The Covid-19 pandemic has severely tested the emergency management capacity of all affected states, having a direct impact on multiple sectors and daily activities. In this context, tools and mechanisms for national and international cooperation were developed and reinforced, both at political and military levels. In Romania, civil-military cooperation played a very important role in the context of the Covid-19 pandemic, showing high adaptability and response. Moreover, the Romanian government, through its Department for Emergency Situations, took advantage of the international mechanisms of assistance to solve unexpected problems during this global emergency, closely cooperating with NATO, the EU, and the World Bank.

The Romanian Department for Emergency Situations is the national point of contact for the European Response Coordination Centre (ERCC) and NATO's Euro Atlantic Disaster Response Coordination Centre (EADRCC). Both ERCC and EADRCC were synchronised in international humanitarian assistance, functioning as two complementary

mechanisms that allowed exchange of information between the EU and NATO as well as increased coordination among member states and their partners. From this point of view, Romania is a fortunate example of a coordinated approach between the mechanisms of the two international organisations.

At the NATO level, Romania has requested NATO's Strategic Air Transport Capability, which operates from the Papa Air Base in Hungary, to conduct an emergency air mission to transport approximately 45 tons of medical equipment from Seoul to Bucharest. At the EU level, the financial advantage of partial or full coverage for humanitarian flights gave Romania the possibility to use its military planes to repatriate and import medical equipment for the strategic stockpile. An important aspect of the repatriation process and the transport of medical equipment was EU support through the reimbursement of transportation costs (i.e. 75% coverage of expenditure through funds allocated to the UCPM or full coverage under ESI).

At the EU level, Romania also contributed to supporting other countries as one of the two countries hosting the medical reserve under rescEU. The medical reserve entered into force in 24 April 2020 and medical protective equipment from the reserve was delivered – using the logistic resources provided by the Romanian Ministry of National Defence and the General Inspectorate for Emergency Situations – to various countries, such as Croatia, Czech Republic, Italy, Lithuania, Montenegro, North Macedonia, Serbia, Spain, and bilaterally to the Republic of Moldova and Ukraine.

At the national level, one of the main weaknesses was the lack of a preparedness culture, which led to increased vulnerability in communities and less resilient societies. To tackle this issue, the Romanian Department for Emergency Situations and the World Bank started to work together to develop a project on behaviour change to identify the social and cultural factors that determine the way Romanian society perceive natural disasters, their level of self-efficacy around preparedness measures, and barriers to adopting preparedness measures. Strategic communication and adequate messages can influence 'individual risk perceptions and risk reduction responses during a crisis like the Covid-19 pandemic. Understanding risks is key to persuading

people and their governments to do something in the face of uncertainty and crisis. They need to know what the risk is, how bad it is, and what they need to do to reduce their risk or help the collective effort' (Weible, 2020, p. 10).

The main pillars of this project are focused on components, such as: (i) *risk perception* (people's assessment about the likelihood and severity of natural disasters); (ii) *beliefs about responsibility* (people's perception of their responsibilities towards themselves, their family and their wider community in preparing for and preventing natural disasters, rather than the expectation that the state will always take a primary role in providing immediate assistance); (iii) *trust* (people's perception of government institutions and the information they provide to the population regarding natural disaster preparedness); (iv) *self-reliance* (people's belief in their own ability to cope with natural disasters, and their ability to adopt preparedness behaviours); (v) *awareness of preparedness requirements* (people's knowledge of the resources and actions required to be prepared for natural disasters).

Over time, Romania has managed to build strong ties with international organisations, both in terms of capabilities and mechanisms for assistance at the NATO and EU level, as well as in terms of innovative approaches, such as the behaviour change research project with the World Bank. This continuous involvement represents a strategic medium and long term vision, having as a main outcome the achievement of an integrated civil protection mechanism at national level. Moreover, Romania took advantage of its membership in international organisations and managed to organise training seminars and a wide range of exercises (including field, tabletop, and virtual/augmented reality exercises) to test its capacities, procedures, and operational reaction, involving observers from NATO, the EU, and the UN, using the toolbox packages that international organisations offer, and sharing best practices with experts and stakeholders from other member states.

In February 2019, the Department for Emergency Situations and the European Centre of Excellence for Countering Hybrid Threats jointly organised a dynamic workshop under the Romanian Presidency of the Council of the European Union that took stock of EU and NATO requirements and methods for civil protection.

The workshop featured a tabletop exercise involving a respiratory virus, the microbiological and epidemiological factors being realistic and based on modern medical knowledge. In this scenario, a highly contagious respiratory virus struck in a situation where the target country and its neighbouring countries were already struggling with forest fires so the national medical capacities had already been pushed to and beyond the limits and respirators and intensive care units (ICUs) were needed for forest fire victims. The effects were further exacerbated by other hybrid operations, such as a cyber-attack against the health sector and disinformation.

Key findings:

- Insufficient stocks of basic and specialised medical materials that would be needed in case of an airborne pandemic and resulting urgent need to pool resources as soon as possible, especially by stockpiling the relevant materials;

- The situation is aggravated by the very complex arrangements and lengthy procedures to step up or even modify the production of these materials in the event of an emergency that is already ongoing;

- The need to plan and be prepared for situations that are inherent to human societies (widespread contagious diseases), even with all the technological and medical progress achieved until now;

- The necessity to improve readiness for a community-level response.

Recommendations:

- Development of common reference scenarios (e.g. for a pandemic) at the EU level while considering expertise from complementing actors/ sectors (e.g. ECDC);

- Expert exchange on methods and tools for risk analysis, data collection and homogenisation, joint planning sessions on risk management capabilities by cross-sectoral expert groups (academia, science, policy, private sector, etc.);

Developing an information/knowledge management toolbox to complement UCPM based on the following needs identified during the tabletop exercise: sharing operational rules, sharing strategies for early warning of the population, sharing best practices for ensuring business continuity of civil protection/ emergency management authorities, sharing best practices on carrying out multi-sectoral lessons learned processes to increase resilience at national and international level. Following the conclusion of the workshop, the key findings and recommendations reflected the present day reality where nobody is prepared to deal with a pandemic – neither international organisations nor member states by themselves. A global strategy has to be built for cooperation on resilience, as resilient societies start with resilient citizens. If international organisations do not work and function well, their member states can be confused and lose access to necessary toolboxes (mechanisms, instruments, and platforms). Thus, it is important to build contingency planning at the national level and to create a framework of common rules for member states at the international level.

2.2 ROMANIA'S COOPERATION WITH THE CIVIL SOCIETY AND PRIVATE SECTOR

At the beginning of the Covid-19 pandemic, an unexpected paradox occurred that had not been anticipated at the global level. Instead of strengthening ties between international organisations and member states, international cooperation actually weakened them, leading to a lack of joint, unified, and homogenous measures at both the European and international levels. In this situation, Romania has tried to identify additional resources at the national level and has been actively involved in cooperation with civil society organisations and the private sector.

This cooperation mainly targeted public awareness campaigns and humanitarian convoys, with the main focus on supporting disadvantaged/marginalised areas and the vulnerable and/or isolated population. Following the AoA methodology and techniques, according to the figure presented above, it can be seen that technology is an engine for social change as well as an enabler that annihilates geographical barriers, optimises procedures, helps societies to grow and become more resilient.

Emerging technologies have played a crucial role during the global emergency generated by Covid-19, especially through innovative solutions that provide an added value in different areas from prevention to preparedness, from mitigation to response. Technology is a challenge but can decisively contribute to saving lives if used in the right way. In order to understand the impact of emerging technologies, mainly in the Covid-19 context, I will further present three examples from the Romanian cooperation with civil society organisations and the private sector: cooperation with SAP Romania, Code for Romania, and Bucharest Robots Start-up.

Cooperation with SAP Romania

The initial goal of the cooperation with SAP Romania was to explore technological solutions for helping the Romanian authorities to better respond to the Covid-19 pandemic using artificial intelligence and robots. One of the proposals generated a pilot project related to a chat bot, the main function of which would be to reduce call loads, especially the load of repetitive questions addressed to the Health Authority Management at the local level. Moreover, there have been discussions regarding a web/mobile app for liaising with family doctors and connect with confirmed cases to increase the efficiency in monitoring their symptoms and their overall state of health.

Technology is an important factor in overcoming the crisis, not only at the economic level but also at the societal level: 'The future has moved into our presence, and we must adapt even quicker than before and find new ways of reaching out to one another. SAP helped its customers adapt to rapidly changing conditions, and provided solutions to directly address many of the issues faced by customers and the broader community caused by Covid-19: understanding and responding quickly to needs, meeting acute sourcing challenges, temporary staffing, managing business travel disruption and remote working' (interview with Josephin Galla, Managing Director for SAP South East Europe & Ukraine). Transformation and adaptation – especially in crisis situations – are required at global level and SAP proactively

helped governments, Romania being a new-entry on a longer list with Bulgaria, Germany, the Netherlands, and the United States[2].

Technology is at the forefront of evolving processes, it is an open door to transforming expectations into actions, on the condition of being used in the right way and for the right purpose.

Cooperation with Code for Romania

The NGO's perspective on using technology and finding digital solutions adapted to new circumstances is characterised as follows: 'technology in itself is not a goal and it is not enough to own the tech, but how you channel its benefits to help communities and societies increase response and resilience capacity. Tech in various forms has always been around and has always been a facilitator of progress. If we take a look at the past 10 years, we will see that civic technology, together with gov tech and social tech, has become more and more essential to healthy societies all over the world. Initiatives, such as Code for America, Code for Africa, mySociety and many more, have dedicated immense efforts to solving social and civic issues through the use of software and also hardware' (interview with Olivia Veraha, Co-founder and Chief Operations Officer at Code for Romania).

Cooperation with tech NGOs, such as Code for Romania in developing a Covid-19 ecosystem based on a comprehensive package of technological solutions, useful for both national authorities and the population, resulted in several apps and platforms: *StiriOficiale.ro* (Official News), *Date La Zi* (Current Data), *Ce Trebuie Sa Fac* (What Should I Do), Diaspora Hub and RoHelp.

[2] A few examples of SAP's contribution to fighting Covid-19 at the global scale by using technology: Bulgaria – a monitoring system developed specifically for the Covid-19 crisis which provides the citizens with continuous information on the Covid-19 situation, but also identifies risk groups through screening questions and manages voluntary offers; Germany – development of a platform at the request of the German MFA on which citizens stranded abroad could indicate their intention to return home, helping the German government to organise their secure repatriation; Netherlands – cooperation between private stakeholders in order to develop the Corona Warn App. United States – helping to set up an emergency hospital in New York, especially by allowing access to the SAP platform to enhance hospital beds procurement and delivery in a fast-paced manner (i.e. procurement of 500 beds and delivery in 30 minutes).

Since its launch, the platform *StiriOficiale.ro* (official news) was considered as the central hub of the digital ecosystem in terms of communication, each news digital product being linked to this one. According to the data centralised by Code for Romania, one in four adults in Romania has used the platform for information. At the same time, the platform *DateLaZi.ro* (current data) provided daily statistics on the pandemic evolution on the national territory. Moreover, the platform *CeTrebuieSaFac.ro* (what should I do) provided useful content for the pandemic period, demystification, advice for parents, information about the pandemic, etc. *Diaspora Hub* represented a platform designed for both Romanian citizens abroad and various entities informal support groups, NGOs and cult entities that were in need. Last but not least, the *RoHelp platform* included small and medium organisations that carried out local actions that needed fundraising during the pandemic. All of the solutions are still up and running and the subscribers database keeps on growing every month.

Furthermore, the Department for Emergency Situations and Code for Romania, with the support of the World Bank, developed the Resource and Volunteer Management App (version 1.0 RVM) application that can be particularly adapted to the Covid-19 pandemic. The application allows inventory management of available resources, maintains a clear situation regarding the quantities, types of materials and places where they are stored, as well as the status of volunteers organised on distinct skills and specialisations. Almost all CSOs have a set of resources, thus human and material resources can be monitored and even used in case of disasters: headquarters, tents, sleeping bags, high-coverage communication channels, shelter facilities, first-aid kits, or even medical personnel or the adequate infrastructure to raise funds and organise donations in kind, humanitarian activities or awareness campaigns.

Cooperation with the Bucharest Robots Start-up

Civil society organisations and the private sector were involved in building modular field hospitals (medical support units) for non-critical or asymptomatic Covid-19 patients. This project resulted in a 'hospital of the future' using various technologies and artificial intelligence to ensure the minimum contact between the infected persons and the medical staff: automatisation of patients triage, connected medical services and

fleet of robots (in charge of air/ground disinfection based on UVC rays, serving at the patient's bedside, discussing with the patient on the Covid-19 effects based on its AI module, providing instructions regarding the dining place, bathrooms, Wi-Fi network and internet password). Robots can help a lot during crisis management situations: 'disinfection robots, cleaning robots, delivery robots, telepresence robots – they can all help humans' (interview with Ana-Maria Stancu, CEO Bucharest Robots, board member euRobotics).

Moreover, technology can help in numerous other ways: monitoring existing processes, generating alerts and repeated scenarios to educate the general public in the context of emergency and/or exceptional situations: 'in all these cases, technologies, such as IoT, 5G and robots can become useful tools in deploying solutions for societies. Moreover, at the EU level, strategies for AI were drafted considering the status quo and current situation. When the pandemics started, the European Commission gathered information about available AI and robotics solutions to fight pandemics and launched several funding opportunities to develop new solutions' (interview with Ana-Maria Stancu, CEO Bucharest Robots, board member euRobotics).

*

Interconnectivity among all stakeholders (international organisations, member states, civil society, private sector) was helpful in fighting SARS-CoV-2 and its consequences. Even if not coordinated and complementary in the first phase, states and international organisations managed to find a common path to advance. In the longer run, it is important to identify lessons learned from Covid-19, work together at all levels and help societies become more resilient. Romania tried to work with local actors at the beginning, to identify back-up measures and activate contingency planning, and later on to use the toolbox packages (mechanisms, instruments and platforms) offered by international organisations to increase its strengths and overcome weaknesses in crisis management.

CONCLUSION

This article presented the concept of resilience seen from the perspective of different lenses in the light of the Covid-19 pandemic, but also tried to answer the research questions presented at the beginning.

Regarding the first research question, '*How can international organisations develop a multi-layered and integrated toolbox in building resilient societies?*', we have learned through this article that resilient societies are at the front line in increasing the level of resilient states and international organisations. The set of approaches, assets, and ambitions of international organisations and their member states became visible relatively late. Problems, such as lack of coordination, decrease of international cooperation, gaps in finding a common strategy, bureaucratic decision-making – all these require the review of resilience ecosystems in times of crisis.

However, the strategic interplay between resilience and Covid-19 managed to find solutions and to limit the general uncertainty, in a balanced approach between strengths and weaknesses. The link of resilience with security (NATO), society (EU), and development (UN) represents an interconnected approach at global level and brings specific layers for each international organisation. Once the communication process started, international organisations have activated their coordination mechanisms and control instruments, and the situation started to considerably improve on the ground (i.e. national and international policymaking, crisis response and management, scientific and technical expertise, exchanges between experts at different levels).

For example, NATO EADRCC and EU ERCC have been working as a resilient toolkit in crisis management, being complementary and synchronised, allowing exchange of information and coordinated responses. It is also important to stress the fact that both NATO and EU provided assistance not only to their member states but also to their partners, being able to cope with pandemic challenges. However, at the UN level, the framework of multilateralism was replaced with unilateral measures, limited or delayed involvement, all of these contributing to put international cooperation in a negative light.

NATO, in its capacity as an integrator during the Covid-19 pandemic, was interested in developing multi-layered mechanisms of cooperation, being mainly focused on civil-military cooperation (i.e. logistic assets and transport capabilities, medical and non-medical support), cross-sectoral cooperation (i.e. seven baseline requirements for resilience), and international cooperation (i.e. partnership, coordination and harmonisation). Civil preparedness and the seven baseline requirements have energised NATO's approach to resilience.

The EU, in its capacity as a multi-nodal integrator during the Covid-19 healthcare crisis, was involved in updating its policies, developing multi-layer measures around the 4P: prevention, preparation, protection, and promotion. Risks require adequate and adapted SWOT and PMI analyses, and we have seen the importance of the UCPM arms through its new instruments, such as rescEU and ESI. The EU's support has been beneficial in vaccines supplies, treatment with authorised medicine, transport of medical teams and patients, training of healthcare professionals in ICU, and building strategic stockpiles, all of which have improved the EU's approach to resilience.

The UN, acting as a facilitator during the Covid-19 global emergency, was concerned with improving communication for better crisis management through the WHO, as well as providing recommended health measures. Moreover, through its PEOPLES Resilience Framework and the UN SDG, the UN is focused on citizens and communities as main drivers of societal resilience. Community-driven solutions and reinforced communities to cope with crisis situations have been acted as a catalyser for the UN approach to resilience.

The second research question, '*To what extent member states can use this toolbox to increase their strengths and overcome weaknesses in crisis management?*, highlighted the transition from the international to the national level, based on a case study of the Romanian strategic response to the Covid-19 pandemic.

The link between crisis management and civil protection should provide an open space for effective cooperation among decision-makers and stakeholders that allows integrated, interoperable and interconnected solutions. Thus, we have observed throughout the case study that

Romanian cooperation with international organisations as well as with the civil society and private sector can lead to timely decisions.

Over time, Romania has managed to build strong ties with international organisations, using all the available international mechanisms and instruments for crisis management, as well as building upon strategic partnerships with civil society and private sector, all of these contributing to innovative solutions and quick responses in the benefit of the population. The challenge is not yet over, however: 'with this greater interconnectivity [...] the policies and practices towards infectious disease outbreaks in the countries of the region, as well as the interplay between regional states and international organisations and institutions, are an important topic for study' (Lo Yuk-ping and Thomas, 2010, p. 448).

To conclude, Covid-19 highlighted gaps and inconsistencies at the level of both member states and international organisations. Even if we identified over this article multi-layered and integrated toolbox packages in building resilience and overcoming crisis management, it is clear that there is a difference between strategy and practice, exercises and real time emergencies and disasters. Nobody was prepared for the current pandemic and most probably it will still take some time before scientific solutions are put in place. However, the main lesson learned is that most of the nations are far away from having resilient societies and this should be their main priority in the future: build a culture of preparedness and contribute to the behaviour change of their populations. This will help prepare for and prevent future epidemics or natural and man-made disasters.

LIST OF ACRONYMS

1.	AI	Artificial Intelligence
2.	AoA	Analysis of Alternatives
3.	CECIS	Common Emergency Communication and Information System
4.	CEO	Chief Executive Officer
5.	CSO	Civil Society Organisation
6.	EADRCC	Euro Atlantic Disaster Response Coordination Centre
7.	ERCC	European Response Coordination Centre
8.	ESI	Emergency Support Instrument
9.	EU	European Union
10.	HILP	High Impact Low Probability
11.	ICU	Intensive Care Units
12.	IoT	Internet of Things
13.	IRCSG	The Industrial Resources and Communications Services Group
14.	MERS	Middle East Respiratory Syndrome
15.	MFA	Ministry of Foreign Affairs
16.	NATO	North Atlantic Treaty Organization
17.	NATO CEPC	NATO Civil Emergency Planning Committee
18.	NATO CPG	NATO Civil Protection Group
19.	NATO JHAFG	NATO Joint Health, Agriculture and Food Group
20.	NATO SPS	NATO Science for Peace and Security Programme
21.	NATO TG	NATO Transport Group
22.	NGO	Non-Governmental Organisation
23.	PEOPLES	Population and Demographics, Environmental/Ecosystem, Organised Governmental Services, Physical Infrastructure, Lifestyle and Community Competence, Economic Development. Social-Cultural Capital
24.	PMI	Plusses, Minuses, Interesting
25.	RES	Resolution
26.	rescEU	European Reserve of Resources
27.	RVM	Resource and Volunteer Management App
28.	SARS	Severe Acute Respiratory Syndrome
29.	SDG	Sustainable Development Goals
30.	SWOT	Strengths, Weaknesses, Opportunities, Threats
31.	UCPM	Union Civil Protection Mechanism
32.	UN	United Nations

33.	UN OCHA	United Nations Office for the Coordination of Humanitarian Affairs
34.	UNDRR	United Nations Office for Disaster Risk Reduction
35.	WHO	World Health Organisation

BIBLIOGRAPHY

Boin, A. and Lodge, M. (2016), 'Designing resilient institutions for transboundary crisis management: A time for public administration', in *Public Administration*, Volume 94, Issue 2, pp. 289–298.

Boin, A., 't Hart, P., Stern, E. and Sundelius, B. (2005), *The politics of crisis management: Public leadership under pressure*, Cambridge University Press, New York.

Bynander, F. and Nohrstedt, D. (2020), *Collaborative crisis management: Interorganizational approaches to extreme events*, Routledge, New York.

Comfort, L., Kapucu, N., Ko, K., Menoni, S. and Siciliano, M. (2020), 'Crisis Decision-Making on a Global Scale: Transition from Cognition to Collective Action under Threat of Covid-19' in *Public Administration Review*, Volume 80, Issue 4, pp. 616-622.

Dalgaard-Nielsen, A. (2017), 'Organizational resilience in national security bureaucracies: Realistic and practicable?' in *the Journal of Contingencies and Crisis Management*, Volume 25, Issue 4, pp. 341-349.

Davies, S. (2008), 'Securitizing infectious disease', in *International Affairs* no. 84, pp. 295–313.

European Commission (2012), *The EU Approach to Resilience: Learning from Food Security Crises*, Communication from the Commission to the European Parliament and the Council, COM(2012) 586 final, Brussels.

European Commission (2017), *A Strategic Approach to Resilience in the EU's external action*, Joint Communication to the European Parliament and the Council, JOIN(2017) 21 final, Brussels.

European Commission (2019), *Civil Protection – rescEU*, retrieved from https://ec.europa.eu/echo/what/civil-protection/resceu_en

European Union (2020a), *The common EU response to Covid-19*, retrieved from https://europa.eu/european-union/coronavirus-response_en

European Union (2020b), *Emergency Support Instrument*, retrieved from https://ec.europa.eu/info/live-work-travel-eu/health/coronavirus-response/emergency-support-instrument_en

Fidler, DP and Draeger, N. (2006), 'Health and foreign policy', in *Bulletin of the World Health Organization* no. 84, p.687.

Giovannini, E., Benczur, P., Campolongo, F., Cariboni, J. and Manca, A-R (2020), *Time for transformative resilience: the Covid-19 emergency,* JRC Science for Policy Report.

Lo Yuk-ping, C. and Thomas, N. (2010), 'How is health a security issue? Politics, responses and issues' in *Health Policy and Planning*, 25(6), Oxford University Press, pp. 447–453.

NATO (2010), *NATO's New Strategic Concept: Active Engagement, Modern Defence*, retrieved from https://www.nato.int/strategic-concept/pdf/Strat_Concept_web_en.pdf

NATO (2017), *The NATO Alternative Analysis Handbook*, retrieved from https://www.act.nato.int/images/stories/media/doclibrary/alta-handbook.pdf

NATO (2020a), *Coronavirus response: NATO Defence Ministers plan for possible second wave of Covid-19*, retrieved from https://www.nato.int/cps/en/natohq/news_176558.htm

NATO (2020b), *Coronavirus response: NATO supports practical scientific cooperation with Allies and partners to enhance Covid-19 diagnosis*, retrieved from https://www.nato.int/cps/en/natohq/news_175619.htm

NATO website, *Resilience and Article 3*, retrieved from https://www.nato.int/cps/en/natohq/topics_132722.htm

NATO website, *Civil Emergency Planning Committee (CEPC)*, retrieved from https://www.nato.int/cps/en/natohq/topics_50093.htm

Official Journal of the European Union (2013), *Resilience and disaster risk reduction in developing countries*, European Parliament resolution on the EU approach to resilience and disaster risk reduction in developing countries: learning from food security crises (2013/2110(INI)), Brussels.

Official Journal of the European Union (2019), Decision (EU) 2019/420 of the European Parliament and of the Council of 13 March 2019 amending Decision No. 1313/2013/EU on a Union Civil Protection Mechanism, L 77 I.

Pirages, D. and Runci, P. (2000), 'Ecological interdependence and the spread of infectious disease', in Cusimano, M., *Beyond Sovereignty: Issues for a Global Agenda*, St Martin's Press, New York, pp. 176–194.

Renschler, C.S. (2013), *The PEOPLES resilience framework: An integrated quantitative measure and modeling of sustainable development and disaster risk reduction*, UNDRR, New York.

Roepke, W-H and Thankey, H. (2019), *Resilience: the first line of defence*, NATO Review.

The North Atlantic Treaty (1949), retrieved from https://www.nato.int/cps/en/natolive/official_texts_17120.htm

The Presidents of the Council and the Commission (2020), *A Roadmap for Recovery; Towards a more resilient, sustainable and fair Europe* (21 April), retrieved from https://www.consilium.europa.eu/media/43384/roadmap-for-recovery-final-21-04-2020.pdf

Trenin, D., Slaughter, A-M, Lehne, S., Biscop, S., Mitter, R., Tocci, N., Möller, A., Hanada, R. and Lisbonne-de Vergeron, K. (2020), 'The Multilateral Order Post-Covid: Expert Voices' in *IIEA*, Foreign Policy Chair, retrieved from: https://www.egmontinstitute.be/content/uploads/2020/06/The-Future-of-Multilateralism-post-Covid_IIEA-Expert-Voices-publication.pdf?type=pdf

United Nations Habitat, *Resilience*, retrieved from https://unhabitat.org/resilience

United Nations website, *Sustainable Development Goals*, retrieved from https://www.un.org/sustainabledevelopment/cities/

Warsaw Summit Communiqué (2016), paragraphs 4 and 73, retrieved from http://www.nato.int/cps/en/natohq/official_texts_133169.htm

Weible, C., Nohrstedt, D., Cairney, P., Carter, D., Crow, D., Durnová, A., Heikkila, T., Ingold, K., McConnell, A. and Stone, D. (2020), 'Covid-19 and the policy sciences: initial reactions and perspectives', in *Policy Sciences*, Springer, Berlin.

Widmalm, S., Parker, C-F. and Persson, T. (2019), *Civil Protection Cooperation in the European Union. How Trust and Administrative Culture Matter for Crisis Management*, Palgrave Macmillan.

Wiig, S. and Fahlbruch, B. (2019), *Resilience from the United Nations Standpoint: The Challenges of 'Vagueness'*, Springer, Berlin.

Wong, B. (2020), 'China's Mask Diplomacy' in *The Diplomat*, retrieved form https://thediplomat.com/2020/03/chinas-mask-diplomacy/

Guiding interview protocol

Galla, Josephin, Managing Director for SAP South East Europe & Ukraine, online interview held on August 29, 2020.

Stancu, Ana-Maria, CEO Bucharest Robots, board member euRobotics, online interview held on August 29, 2020.

Veraha, Olivia, Co-founder and Chief Operations Officer at Code for Romania, online interview held on August 29, 2020.

IMPROVING POLICING THROUGH TECHNOLOGY: A COMPARISON OF DRONE CAMERAS AGAINST TERRESTRIAL SCANNERS IN TRAFFIC ACCIDENT DATA COLLECTION

Jaanika Puusalu, PhD
Estonian Academy of Security Sciences
Internal Security Institute
Junior Research Fellow

Andres Mumma
Estonian Academy of Security Sciences
Head of the Drones and Remote Sensing Centre

Keywords: traffic accidents, drones, data collection, geo-referencing, photogrammetry

ABSTRACT

This article presents the results of a field test of drone technology which is being used in the collection of traffic accident data as conducted by the Estonian Academy of Security Sciences in September 2019. The experiment is part of a larger research project which is investigating the viability of the use of new forms of technology in traffic police work, especially drone cameras. Drones have shown that they have the potential to support and enhance traffic accident data collection, and can therefore greatly enhance the legal processing of accident scenes. Additionally, drones are able to capture data at a comparatively quicker rate than are manual methods. Further investigation is required, however, to determine whether data that is collected by drones is sufficiently accurate for the purposes of carrying out measurement checks at accident sites.

The aim of the field test being presented here was to compare the accuracy and speed of data collection using the terrestrial scanner, a Leica C10 ScanStation, and a quadcopter drone, the Matrice 210v2 with 15 mm RGB, 45 mm RGB, and thermal infracted 13 mm cameras. Measurement accuracy was calculated in terms of data, both with and without geo-references, via the use of photogrammetry. Taking terrestrial scanner measurements as a benchmark, the experiment found the following: i) when drone data was geo-referenced, the difference between the benchmark and those measurements that were based on drone camera data ranged from 6.7–7.5 cm; without geo-referencing the error or difference was significantly higher, reaching at least 2 m; ii) when a local scale bar measurement was used, camera data accuracy remained high even without the data being geo-referenced.

Although geo-referencing can improve accuracy, the additional software and also hardware requirements add additional time and the requirement for a level of skill to the job of data processing. Results with local scale bar measurement, however, indicated the likelihood that geo-referencing may not be required to maintain accuracy rates. When considering these results, the article concludes that drone technology bears further study as an alternative to the currently-used manual methods.

INTRODUCTION

This article presents the results of a field test involving drone technology,[1] specifically in terms of the collection of data where it is related to the scene of a traffic accident, as conducted by the Estonian Academy of Security Sciences in September 2019. This field test focussed on the data collection process in low-light conditions, using an accident scenario in which a pedestrian has been hit by a private motor vehicle, with the accident having taken place in an urban setting. The field test is part of a larger area of research which is investigating the viability of new forms of technology in traffic police work, especially in the form of drone cameras, and how they may serve to complement existing accident scene documentation practices, especially in terms of measurements being taken by the use of photogrammetry. Currently, accident scene measurements are taken using manual methods, and the adoption of new forms of technology requires an assessment of that technology's use value, including a comparison of accuracy levels and speed against the current methods.

Drone photography, including photogrammetry via drone imagery, has shown itself to have the potential to be able to support and enhance aspects of data collection at the scene of traffic accidents, including the possibility of being able to improve the speed at which data is collected at the scene, as well as allowing the possibility of being able to re-visit and re-measure accident scenes after the initial measurements have been taken. In respect to this second point, the implementation of drone technology also has the potential to improve the accessibility of data for the legal processing of the scene of traffic accidents. Having said that, the usage value of drone photography and drone-data-based photogrammetry in traffic accident scene investigations, including the ability to assess data validity and measurement accuracy, has not fully been established and

[1] As a note regarding terminology, this article is referring to drone technology (or drones, in short), where the drone is 'an unmanned aircraft or ship that is guided by remote control or onboard computers' (Merriam-Webster, 2020). In existing research, drone technology is often also referred to as 'unmanned aerial systems' (UASs). UASs include an unmanned aerial vehicle (UAV), a ground-based controller, and a communications system between the two. This article considers these two ways of referring to the technology to be broadly equivalent, and so the use of these terms is largely interchangeable.

is still subject to testing. Whilst drones have generally proven to offer a rapid solution in terms of data collection, research questions remain regarding whether the speed of data collection may come at the cost of data accuracy, as well as questions remaining regarding the best method to be used for collecting data via drone which could further be used for photogrammetry. The field test described in this paper goes some way towards addressing these questions.

In that light, Section 1 introduces the context within which is located the broader research project to which this paper contributes. Section 2 describes the methodology used in the field test (2.1), and the results for that field test (2.2). The article concludes with a brief analysis of the relevance of those results within both the local and broader research context, including a discussion of further lines of research that have been indicated by the results of the field test.

1. RESEARCH CONTEXT

A significant barrier in terms of the uptake of specific new forms of technology in law enforcement practices, even for forms of technology that have widely been discussed as potential complements to current law enforcement practices, is a lack of research that serves to confirm the reliability and usage value of the relevant forms of technology. One such area, with which the field test described here is concerned, is data collection and measurement at the scene of a traffic accident.

The practice of manually carrying out data collection at the scene of a traffic accident, and especially the measurement of accident scenes, is common around the world. However, this approach is both time-consuming and labour-intensive, which in turn can have indirect negative consequences. Along these lines, research that has been conducted by the US Department of Transportation, and the National Highway Traffic Safety Administration (Blincoe *et al,* 2015), indicates that service providers can incur significant monetary costs through increased fuel usage and time lost due to an accident scene being closed off so that manual data collection can take place. Studies by Dukowitz (2020), Kamnik et al (2019), and the Purdue University (Sequin, 2019), indicate that traffic jams and delays that result from an accident scene investigation can lead to secondary accidents; with the Purdue study finding that secondary crashes increase by up to a factor of 24 during the time in which law enforcement officials are collecting data. Similarly, Dukowitz indicates that the possibility of a secondary crash occurring increases by 3% for every minute that the scene of an accident is sealed off, whilst law enforcement officials and towing and recovery personnel are themselves most vulnerable during that same period (Dukowitz, 2020).

In addition to these costs in terms of time and labour, as well as the physical threat to human life, the common methodology of using a tape measure or a measuring wheel, with manual note-taking, and the use of handheld cameras to document the scene, are all practices that are prone to human error (see Shinar *et al,* 1983; similarly, see also Griffard, 2019, p 53, which shows that attention has been draw to potential problems

both in terms of erroneous data collection and data insertion when it comes to a criminal investigation that makes use of the data).[2]

Despite these apparent issues with manual data collection and measurements at the scene of an accident, few technological alternatives have been considered as being possible complements to existing practices or as ways of enhancing this area of law enforcement (see, for example, Pagounis *et al,* 2006; Osman & Tahar, 2016). Reasons for this include the resilience of the current methodology in the face of various environmental conditions, such as wind, rain, or low levels of lighting, plus which the ease of use of the relevant tools – the way in which they can be used and their levels of reliability – is somewhat robust, and has a comparatively low level of expertise required when it comes to processing the data that is collected. No additional personnel are required for such data processing (for an in-depth analysis of the conditions in which drones could be used, see Padua *et al,* 2020). Moreover, the current methods provide a degree of standardisation in the data collection process across international borders with relative ease (for a European initiative as an example, see SAU – Urban Accident Analysis System, 2007).

Two forms of technology that a growing body of research is testing and assessing as potential complements to the existing manual practices involve terrestrial laser scanners and drone technology. Of particular interest and emphasis within this research is the possibility of using such forms of technology to make possible the process of taking measurements at scenes of accidents to be conducted via photogrammetry.

Terrestrial laser scanners send a laser beam towards numerous points on three-dimensional objects, measuring the distance between the collected data points and the equipment itself. The data produced by this can, in turn, be used to generate a point cloud which, with the use of the appropriate software, is suitable for topographical mapping and spatial analysis (Oguchi *et al,* 2011). Additionally, this model can allow officials to effectively re-visit and re-measure the site at a later date. The scale of the speed and accuracy of point cloud creation – as reported by Oguchi et al (2011) – is between 10^4–10^6 points per second with an accuracy of 10^{-1}

[2] The authors recognise that human error may occur in part as a result of external factors such as, for example, rapidly changing weather conditions, low-level lighting, and so on.

to -10^0cm. In this light, there is evidence (Kersten *et al,* 2008) that laser scanners have an exceptionally high level of accuracy of measurement.[3] In relation to this, there has already been some uptake of this technology in traffic policing practice in the USA (such as, for example, by the North Carolina Department of Transportation, 2017, p 3),[4] and there have been further suggestions that scanners could be employed in crime scene investigation to reach and record points of a crime scene that a standard camera cannot (Tedinnick *et al,* 2019). Barriers to any wider adoption of this technology, especially in traffic policing, however, involve the relatively complicated nature of the technology and the comparatively high level of expertise that is required when it comes to processing the resultant data (although, as Rosell-Polo *et al,* 2019 point out, there is a growing number of user-friendly software applications that provide enhanced opportunities to use the data). In addition, laser scanners are expensive and are better suited for use in areas with less vegetation and a flat surface (Guisado-Pintado *et al,* 2019).[5]

Currently, the primary use of drones at traffic accident scenes, especially in the USA where they are most widely used, has been in terms of providing additional documentation of the accident scene in the form of photographs (especially aerial photographs) that can later be used in the investigation process (Bergal, 2018; Eyerman *et al,* 2018; John Hopkins University, 2018).[6] In light of the limitations that have been mentioned when it comes to employing laser scanners in traffic policing, there is now a growing body of research into the potential shown by drone technology – in combination with photogrammetry software – to also be

[3] Every terrestrial scanner has a defined margin of error that is confirmed by the manufacturer. The scanner being used in this field test was confirmed to have a 4mm margin for error.

[4] The Leica C10 ScanStation model terrestrial laser scanner has been tested for police use in Estonia, and is in some instances also used for 3D modelling. However, due to the absence of a certified methodology for carrying out measurement duties at the scene of a traffic accident, it cannot be used in taking measurements at accident scenes.

[5] There is a growing body of research (especially that which has been considering the use of technology in terms of vegetation, snow, cliffs, etc, when it comes to monitoring and analysis), which has been investigating the simultaneous use of drone technology and TLSs as complementary forms of technology, with drones providing better access, and scanners greater accuracy (see, for example, Cooper *et al,* 2017; Bartoš *et al,* 2019; Yakar *et al,* 2014; Šašak *et al,* 2019).

[6] In a survey conducted in the U.S in March 2019., it was reported that drones are also being used for surveying work, public education and outreach work, emergency response work, and daily traffic control and monitoring, as well as for scientific research and when inspecting high-mast light poles (Bergal, 2018).

able to provide assistance when it comes to data collection and taking measurements at scenes of accidents. One comparative strength of this form of technology is the possibility of being able to attach more than one type of camera to a single drone, thereby providing a greater variety of data to be collected.[7] Additionally, drones are comparatively easy to operate, as well as cheaper to acquire and maintain than are terrestrial laser scanners (Kamnik *et al,* 2019; Perez *et al,* 2019). It is also suggested that the ability to operate the drone from the roadside when taking measurements on site may contribute to the increased safety of the officer who is responsible for operating the drone (Queensland Police, 2019). Finally, the technology may deliver additional value to current practices by enabling the re-measurement of the scene of the accident without it needing to be revisited, as well as allowing for views of the scene of the accident that would not be possible otherwise (such as in terms of providing an overhead 'bird's-eye' view). Employing drone technology in the collection of data from scenes of accidents is limited by weather conditions and the physical features of the specific site of the accident. However, the aspects of the technology that are mentioned above suggest that it may, nonetheless, have significant advantages over terrestrial scanners as a complementary method to existing practices.

That said, there are a number of concerns with the employment of drone imagery via photogrammetry that have so far curbed their use in terms of measurement purposes. Firstly, the camera being used needs to be suitably calibrated so that any data that is collected is not distorted in any way. This calibration, in turn, demands proper flight planning. Experiments that have been conducted by Su et al (2016) do, however, show that a rapid mapping system could be developed that would be suitable for these purposes. Secondly, different cameras and data collecting altitudes can provide photographs that are of differing levels of quality (which is calculated based on the number of pixels in each image), which can distort the size of objects, and their edges, and make the taking of measurements somewhat difficult. Field tests that have been conducted by Jurkofsky (2015) used circular targets for reference in an attempt to overcome this limitation, but that research suggests that the accuracy of photogrammetry can be compromised if such reference targets are not

[7] In the field test being reported in this paper, for example, three different cameras were used on one drone.

used. Furthermore, when using drone camera photos for photogrammetry, the margin of error for the measurements needs to be established separately for each individual scene of accident. This contrasts with laser scanner imagery where the margin of error for measurements that are carried out via the scanner is pre-established by the manufacturer. One approach to overcoming this problem, and one which is already in use, is to georeference the images and any objects that are captured on the images. Using GNSS, this method situates the points at which the drone image is taken onto a world map. This geo-referencing can be carried out either with designated points marking the area at which the data is collected or with the built-in technology of the drone that is being used to take the pictures. The distance between the objects on the photograph, the length of objects, and so on, can be measured according to the designated points (in terms of the position of the point cloud) on the world map and the distance between those points.[8] An alternative is to use a local object of a specific size as a benchmark measure. It is the viability of this process as well as that of the geo-referencing approach that the current research is intended to assess.

Taking all of these issues into consideration, a significant barrier to the adoption of this measurement technology is the lack of evidence that the combination of drone technology and photogrammetry software can provide measurements that are of sufficient accuracy for the purpose of traffic policing and scene of accident analysis (John Hopkins University, 2018, p 57). Two current articles that address this gap are Padua et al (2020), and Kamnik et al (2019). Both of which take the similarity of data results that have been collected by means of conventional methods and those which have been collected using drone technology to be indicative of the feasibility of drone technology for use in traffic accident investigations. It is to this short list of research into accuracy that the field test described here contributes, with a specific focus on the local law enforcement context in Estonia in which the field test was conducted.

Police involvement in traffic accidents (which involve motor vehicle-related collisions) in Estonia is required when a person is harmed or when the parties involved in the collision and/or the owners of other objects that have been involved and damaged in such a collision are

[8] For the methodological concerns see, for example, Zhou *et al,* 2017; Oniga *et al,* 2020.

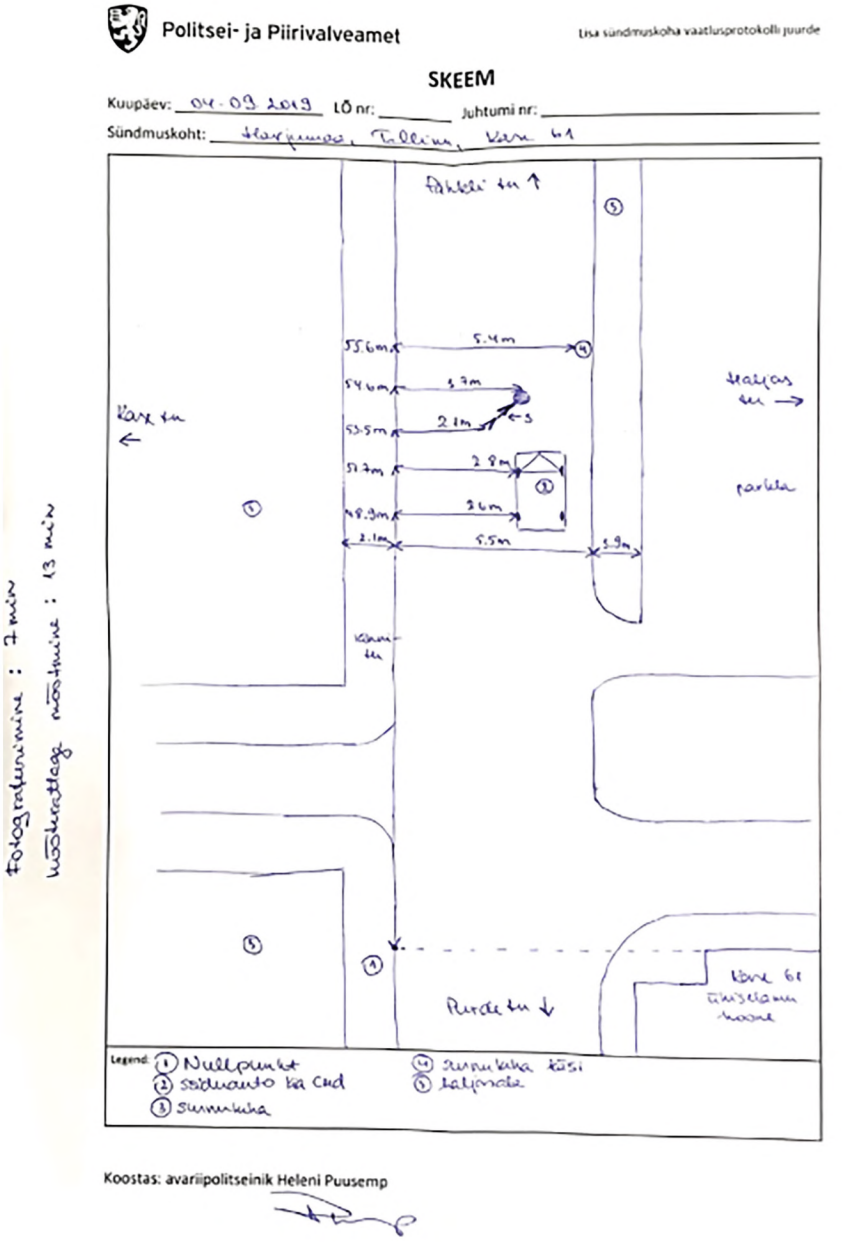


FIGURE 1: Data collection from the traffic accident – initial report at the scene of the accident, produced via the field test.

unable to agree upon the amount of damage that has been done and/or which party is responsible for the accident.[9] In keeping with practices in other countries, accident site data in Estonia is collected manually. Manual data collection precludes the ability to re-create or re-measure the scene of the accident. Therefore, it is of crucial importance that any data which is collected at the scene be as comprehensive as possible. This involves producing an accurate representation of the scene which is suitable for subsequent investigative work in the office and an analysis of the accident. In this light, manual data collection in Estonian traffic policing includes the task of measuring the relevant features of the accident site and providing a schematic representation or memo drawing of the scene (as illustrated in Figure 1). Having conducted this process, the police officers involved will return to their office to draw up a more detailed image of the collision site (a process that is illustrated in Figure 2), which provides the primary material for the investigation, in addition to photographs from the scene of the accident and statements from the parties that were involved in the accident.

In line with earlier comments, the process of carrying out manual data collection and accident site measurement which is currently followed in Estonia is somewhat time-consuming, while potentially also leading to subsequent issues with traffic management – including secondary accidents – and is prone to human error, particularly so with large or complex accidents where producing the detailed plan that is required for the subsequent investigation can be extremely complicated.[10] In addition, a pressing underlying issue that is specific to Estonia is the bearing of demographic changes in a broader sense on current policing practices, where a decreasing population is predicted to lead to a significant reduction in the working age population and, so too, to potential shortfalls in policing staff levels (Ministry of the Interior of Estonia, 2020; Ministry of the Interior of Estonia, 2019). At the same time, a decrease in the relative

[9] In March 2020, Statistics Estonia (Statistics Estonia, 2020a) reported that in 2019, there were a total of 1,406 traffic accidents reported, which means an average of 118 a month and four a day; according to the Estonian Road Administration, by 1 September 2020, there have already been 889 traffic accidents in this year involving human victims (The Republic of Estonia Road Administration, 2020).

[10] When it comes to secondary traffic accidents, the authors recognise the difference in the scale of road traffic in the USA (where the primary body of research originates that is referenced in this article) and in Estonia, but consider the aforementioned concerns regarding the safety of law enforcement officers, etc, to be a pressing concern in Estonia nonetheless.

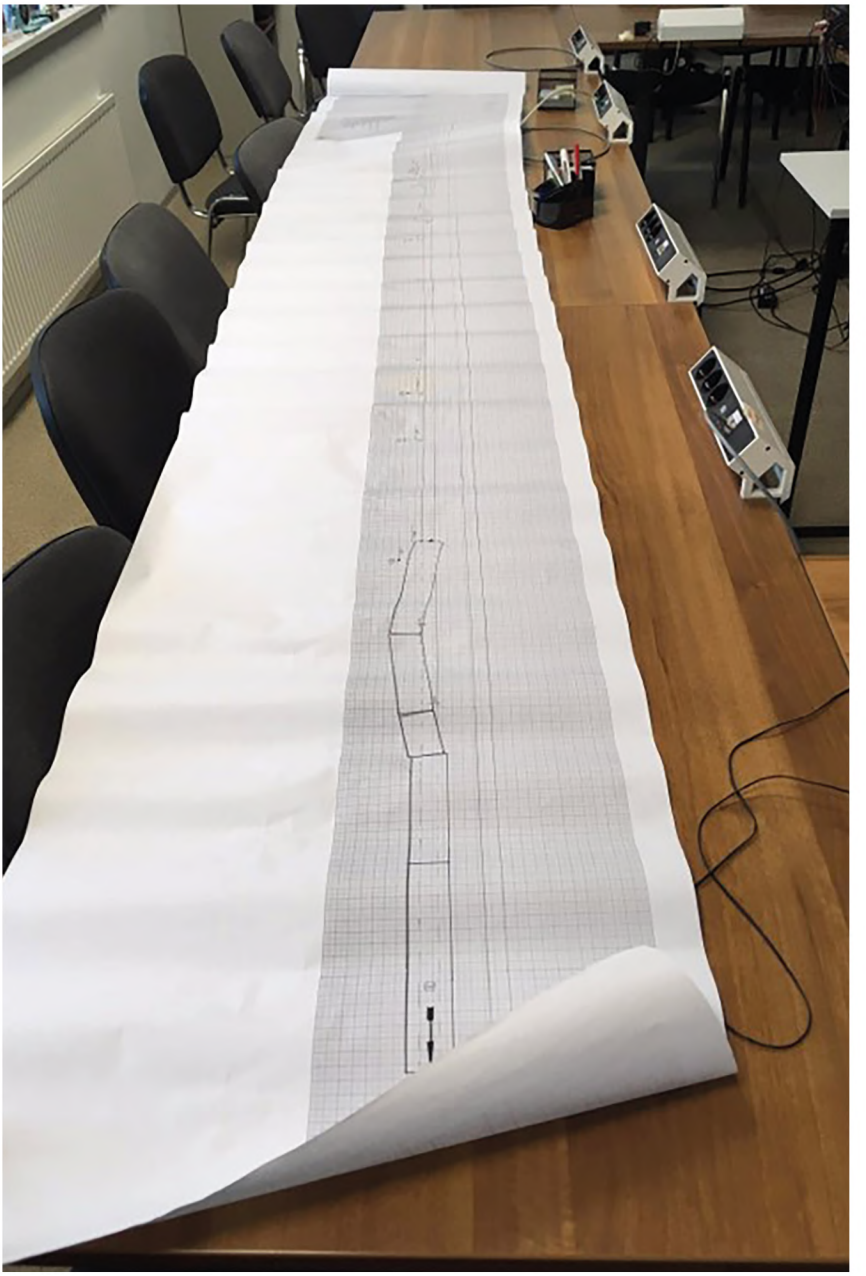


FIGURE 2: Traffic accident report – detailed report, drawn up in the office according to the initial report from the scene of the accident (the report shown involves a rail accident that took place in Raasiku in 2014).

working age population of Estonia need not result in a similar change to the driving population. The population in Estonia, as in Europe more generally, is aging with corresponding rises in life expectancy levels. In line with this trend, it is to be expected that in the future the share of the population that is eligible to drive will continue to increase (Eurostat, 2019). Related to this, economic growth and improving economic welfare has resulted in continued growth in the number of passenger cars being sold in Estonia, with the last five years alone seeing the number of privately driven motor vehicles on the road increasing by 100,000 (Statistics Estonia, 2020b). These demographic and economic shifts may then produce reductions in the number of available traffic police at the same time as there is an increased need for traffic policing, including being able to respond to and investigate scenes of accidents.[11] Considering these shifts, it is vital to policing across the board in Estonia that policing practices be modernised when and where that is suitable and possible – including in the provision of traffic policing.[12]

Within the local context described, the Estonian Academy of Security Sciences launched a research project in 2019 which aimed to assess the potential of employing photogrammetry that can be facilitated by drone along with the process of collecting data via drone as an additional means of measuring details at traffic accident sites. To do so, this ongoing project is conducting a series of field tests,[13] which will compare the image quality of various cameras that are attached to drones which are being employed at a specific accident site to test the efficacy of using (drone) cameras in different lighting conditions,[14] while also testing the efficacy of using (drone) cameras in different settings,[15] and in simulated scenarios,[16] and to analyse the accuracy of measurements that are taken via photogrammetry with and without geo-referenced data. In the remainder of

[11] Thanks are given here to an anonymous reviewer for pushing the need to discuss both aspects of the significance of demographic and economic changes.

[12] The authors take into consideration the possibility that the technological solutions being tested here may be of limited use in Estonia due to the local weather conditions, the density of the population, the large number of rural roads, and other local factors.

[13] At the time of writing, seven field tests have been conducted.

[14] Field tests are conducted in daylight as well as under low-lighting conditions, both with additional lighting and without.

[15] Some field tests simulate built up urban areas, others rural settings and/or larger roads.

[16] Some simulations model accidents in which a pedestrian is hit, while others simulate collisions between cars.

this article, the findings from one field test are presented, which took place on 5 September 2019 on the premises of the Estonian Academy of Security Sciences in Tallinn. The aim of this specific field test was: i) to compare the accuracy and speed of data collection by a specific model of terrestrial scanner and a quadcopter drone which was equipped with RGB and thermal infracted cameras; and ii) to compare the accuracy of the drone data measurement process via photogrammetry with and without geo-referenced data. In the next section (2.1), the methodology used to conduct the field test is described, and in 2.2, the results of the test are presented.

2. FIELD TEST

2.1 METHODOLOGY

The aim of the field test being presented here was to compare the accuracy and speed of data collection using the terrestrial scanner, Leica C10 ScanStation, and the Matrice 210v2 quadcopter drone with 15 mm RGB, 45 mm RGB, and thermal infracted 13 mm cameras. The field test was conducted in low-light conditions during the early hours of 5 September 2019 on the premises of the Estonian Academy of Security Sciences in Tallinn. The field test simulated a densely-built urban area in which the scene of the accident is surrounded by buildings, posts, wires, and other components of a built-up infrastructure. The simulated accident involved one private motor vehicle and a pedestrian, with the latter being represented by a life-size dummy that was employed at the scene of the accident to simulate someone who had been hit by the vehicle, and was now lying in the road a couple of metres in front of the vehicle.

Data gathering was conducted using a Leica C10 ScanStation terrestrial scanner and a Matrice 210 v2 quadcopter drone with 15 mm RGB, 45 mm RGB, and thermal infrared 13 mm cameras. Data was geo-referenced using the RTK GNSS Trimble Catalyst DA1 service with a 10 cm accuracy. For drone data processing and ready-to-use data product development, use was made of the Agisoft Metashape photogrammetry software; CloudCompare software was used for terrestrial scanner data merging. On-scene lighting was provided by two of the police department's portable lighting equipment units, a Solaris Duo 40,000 Lumens Rechargeable LED Lighting System.

Accordingly, five different ready-to-use data products were produced. The first was a handwritten sketch of the scene of an accident (data product-0) in which important measurements were described (see Figure 1). In addition to the sketch, following the data gathering protocol for an accident site, the scene of the accident was photographed using a handheld camera. As with the conventional process, the data collection process from the scene of a road traffic accident is complemented with a more detailed sketch on millimetre paper which will be drawn later (see Figure 2). The measurements that were taken in this process were done using a handheld measuring wheel and were rounded to the nearest tenths of a decimal place, e.g. from 2.11 m to 2.1 m (see Figure 1).

In addition to the manually-produced data product, a Leica C10 ScanStation laser scanner was used to gather data to create a high accuracy point cloud that was later used as the benchmark when it came to comparing the accuracy of drone camera data against the manual product.[17] Data product-1 was generated with the data that had been obtained by means of the laser scanner (the maximum scope for error for the Leica

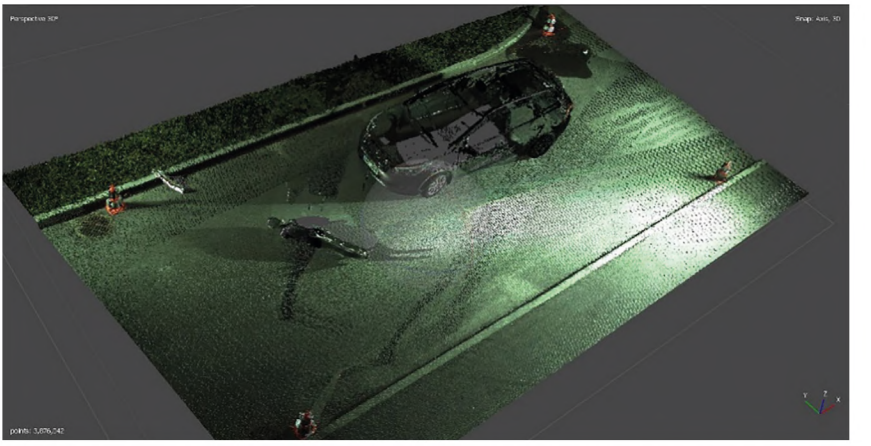


FIGURE 3: A Leica C10 laser scanner point cloud, with benchmark data that has been geo-referenced using RTK GNSS.

FIGURE 4: A 15 mm focal length RGB camera point cloud and orthomosaic, geo-referenced using RTK GNSS.

[17] The use of laser scanner measurements as a benchmark is in keeping with the methodology used in similar research from other countries, such as Jurkofsky, 2015; Kamnik *et al*, 2019.

C10 scanner is 4 mm if the distance being measured is geo-referenced using the aforementioned RTK GNSS (see also Figure 3)).

The second data product (data product-2) and the third (data product-3) were point clouds and orthomosaics that were derived from drone data from the 15 mm and 45 mm focal length RGB cameras. Both of these

FIGURE 5: A 45 mm focal length RGB camera orthomosaic and point cloud, geo-referenced using RTK GNSS.

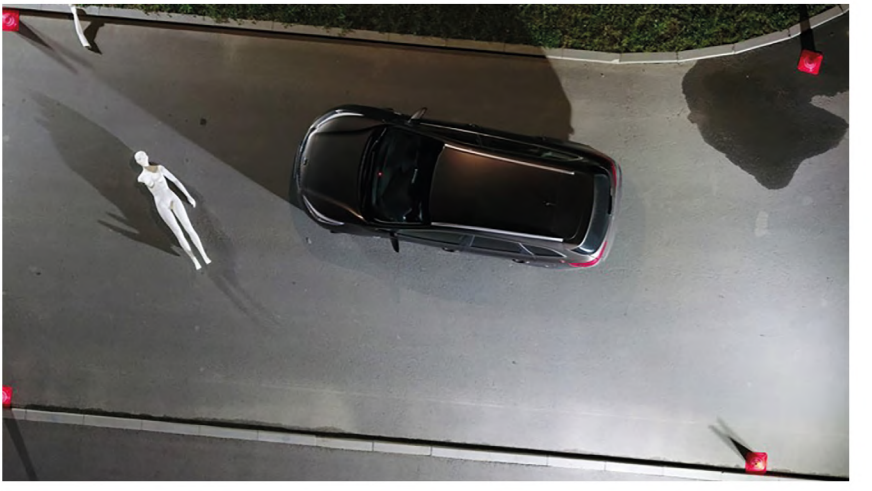


FIGURE 6: A 45 mm focal length RGB camera point cloud, geo-referenced using a scale bar.

data products were also geo-referenced using RTK GNSS (figures 4 and 5). The fourth data product (data product-4) was also derived from the 45 mm focal length RGB camera on the drones, but this was geo-referenced using only the drone's on-board GNSS which has a level of accuracy up to 1.5 m (Figure 5). The fifth data product (data product-5) is identical to the fourth apart from its being geo-referenced with a scale bar (Figure 6).

Once generated, the five ready-to-use data products were then compared, being assessed with a focus upon accuracy and the speed of data collection. The accuracy of the data products that were produced via the use of the drone (data products 2, 3, 4, and 5) was assessed by way of two different methods, both of which have been used in prior research to assess the available options in terms of the use of drone imagery in measuring road traffic accident scenes via photogrammetry. One method was to assess the accuracy of geo-referenced data products (data products 2, 3, and 4) against the benchmark terrestrial scanner measurements (data product-1) in a global context. For the purpose of this assessment, the CloudCompare software was employed, with calculations made for how far the neighbouring points from each of the relevant data products (i.e. the point clouds) as derived from drone data were from the benchmark point cloud that was generated from the terrestrial scanners. The second method was used to assess the accuracy of data product-5, by employing a local scale bar on the image for subsequent measurement.

2.2 RESULTS

The results represented in Table 1 show the time taken to gather the measurements that were used to generate each data product. The results show that using just a drone alone with its own geo-referencing equipment takes significantly less time when it comes to generating a data product than does manual measurement, a laser scanner, or using additional geo-referencing technology. The same speed can also be achieved as when using a drone's built-in geo-referencing technology when using a local scale bar to produce the data product. As shown by the field test results that are presented in Table 1, whilst the drone flight for data gathering takes the same amount of time (five minutes) whether or not the data is geo-referenced, the time taken in setting up the RTK GNSS equipment

TABLE 1: List of ready-to-use data products that were produced as part of the current field test and the time taken to produce each of them.

Data product	Data product name	Time	Place
0	Measuring wheel measurements and photographing	20 minutes	II
1	Terrestrial scanner	50 minutes	III
2	Drone and 15 mm RGB camera, with RTK GNSS geo-referencing	20 minutes	II
3	Drone and 45 mm RGB camera, with RTK GNSS geo-referencing	20 minutes	II
4	Drone and 45 mm RGB camera, with drone GNSS geo-referencing	5 minutes	I
5	Drone and 45 mm RGB camera, with scale bar geo-referencing	5 minutes	I

for geo-referencing purposes increases the data collection time by as much as fifteen minutes. The use of a terrestrial scanner is significantly more time-consuming than the other methods that were used in the field test.[18] The last column in Table 1 ranks the data product in terms of product creation speed.

The remaining results describe the percentage of drone data for each data product that is within, respectively, 5 cm, 10 cm, or 15 cm accuracy of the benchmark product. For data product-5, the assessment was carried out in a two-dimensional setting with the benchmark data being employed in this case coming from those measurements that were carried out using a handheld measuring wheel and a measuring tape. The model was referenced using one measurement – the height of the dummy – and its accuracy was assessed via the use of four independent distances that were measured with a measuring wheel. The results describe how close (in terms of metres) were the distances that were measured via the drone's data model to the benchmark measurements from the measuring wheel.

Figure 7 describes the accuracy assessment of data product-2 against the terrestrial scanner data. The results show that approximately 80% of the drone data has a margin of error that is less than 10 cm, and 95%

[18] The authors recognise that newer terrestrial scanners are significantly quicker in terms of taking the measurements and providing the relevant data for the data product than is the scanner used in the field test (the latest technology can take around fifteen minutes to gather the relevant data).

of it that is less than 15 cm. Figure 8 describes the accuracy assessment for data product-3 against the terrestrial scanner. As illustrated by the data presented in the figures, the results for data product-3 are similar to those for data product-2, with an average error for product-2 being 6.7 cm and an average error for product-3 being 7.5 cm, a difference that is not statistically significant in the current context (it can be noted that data product-3 has a greater number of points and pixels and so generates a higher resolution representation of the scene than does product-2; however, this has no bearing upon the results of the field test).

Figures 9, 10, and 11 describe the accuracy of data product-4. These figures reveal a significant loss in accuracy when only the drone's onboard GNSS device is used, in contrast to data products-2 and 3, both of which are geo-referenced using RTK GNSS. The average margin of error for data product-4 which uses only the onboard GNSS equipment is 4.81 m, whilst data products-2 and 3, which were geo-referenced using separate units, had margins of error that were only between 6.7 cm and 7.5 cm. This 4.81 m average margin of error can largely be explained by inaccurate elevation data, for which the average margin of error is approximately 4 m. However, even when limited to two-dimensional data and so excluding the elevation data, the margin of error is approximately two metres

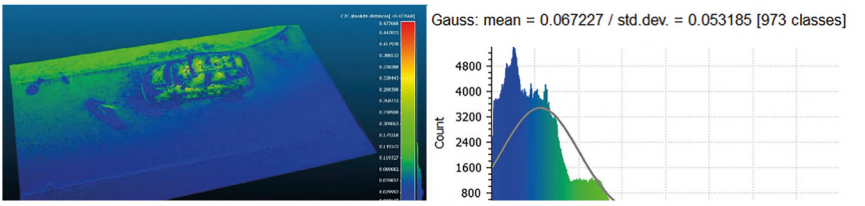


FIGURE 7: An accuracy assessment of a 15 mm focal length RGB camera point cloud (data product-2, RTK GNSS geo-referenced), against terrestrial scanner benchmark data.

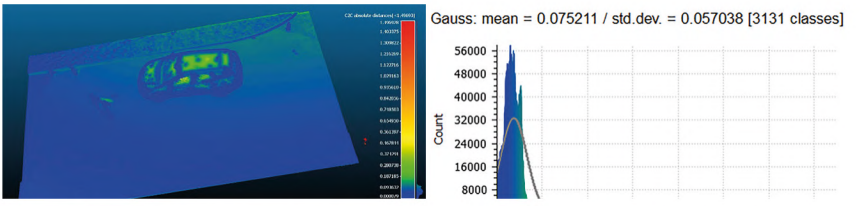


FIGURE 8: An accuracy assessment of a 45 mm focal length RGB camera point cloud (data product-3, RTK GNSS geo-referenced), against terrestrial scanner benchmark data.

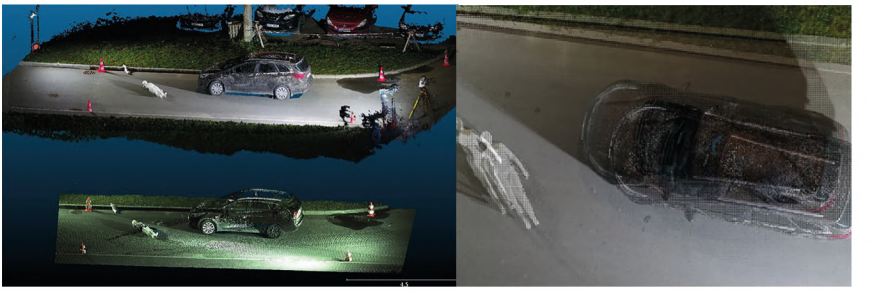


FIGURE 9: An accuracy assessment of a 45 mm focal length RGB camera point cloud (data product-4, geo-referenced using the drone's onboard GNSS), against terrestrial scanner benchmark data.

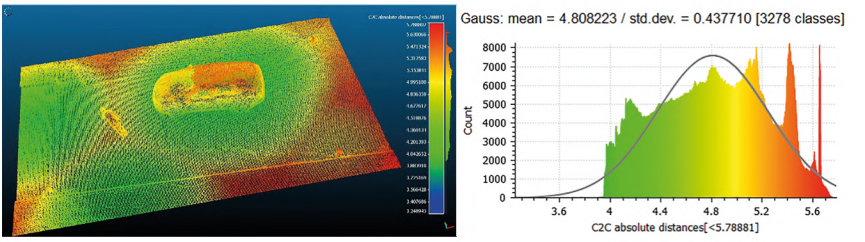


FIGURE 10: An accuracy assessment of a 45 mm focal length RGB camera point cloud (data product-4, geo-referenced using the drone's onboard GNSS), against terrestrial scanner benchmark data in the three-dimensional direction (x, y, and z).

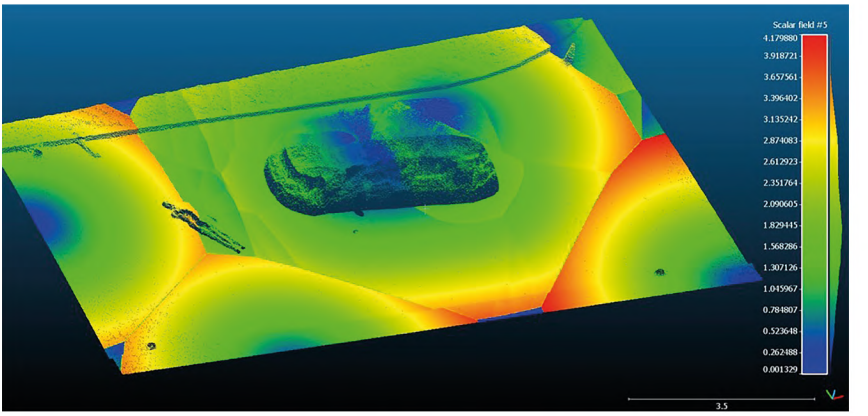


FIGURE 11: An accuracy assessment of a 45 mm focal length RGB camera point cloud (data product-4, geo-referenced using the drone's onboard GNSS), against terrestrial scanner benchmark data in the two-dimensional direction (x and y).

(Figure 11). This means a figure that is around 25 times higher than those for data products-2 and 3.

Figure 12 describes data product-5. This is created from the inaccurate GNSS drone data that was employed in the production of data product-4 but which has been geo-referenced using a local scale bar (a control scale bar) with only one measurement – the dummy – taken by means of measurement tape (1.81 m). In the global geographical context, data product-5 is inaccurate to the same average margin of error as data product-4 (4.81 m). However, when accuracy is assessed without geographical context, and taking into consideration only those measurements that have been taken from the local scene of an accident (i.e. involving only the local context), it can seen that the model measurements that were taken of the dummy exhibit no margin of error at all. That is, the photogrammetry software reports the dummy to be as tall as it was actually measured with the tape measure: 1.81 m.

Taking the dummy's height as a local scale bar, data product-5 includes a further four measurements of distance which were taken at the test site. These additional measurements, which mimic the manual measuring process (data product-0), are not initially geo-referenced, thereby avoiding the accuracy problems that occur with the drone's built-in GNSS system. Accordingly, as the results show, the average margin of error in terms of measurements taken using the local independent scale bar is 8.8 cm. This is only slightly less accurate than measurements that were taken using geo-referenced data in data product-2 and 3, where RTK GNSS was used for geo-referencing. There the respective errors that could be identified were at 6.7 cm for data product-2 and 7.5 cm for data product-3.

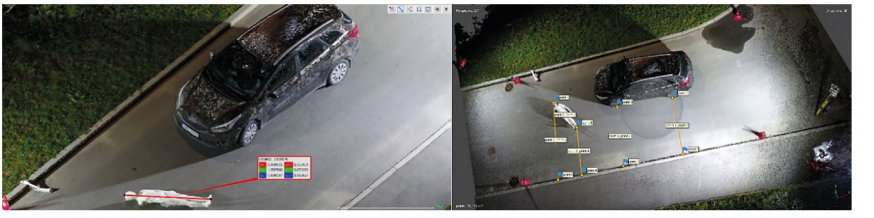


FIGURE 12: A 45 mm focal length RGB camera point cloud (geo-referenced using a scale bar), showing the measurement of the control scale bar (on the left) and the check scale bar (on the right).

Table 2 further presents the results of measurements that were taken using drone imaging (data product-5), using control and check scale bars and comparing these results with the manual measurements that were taken by the traffic police (data product-0). As the results that are presented in the table show, the distances that were measured for data product-5 using the local scale bar (a dummy with a height of 1.81 m) which are presented in the second column, and the measurements that were recorded for data product-0, which are presented in the third column, show a difference in measurements, ie. a margin of error when comparing product-5 to product-0 of up to 10cm. However, the average margin of error when comparing the manual measurements that were taken with the use of photogrammetry was at 8.8 cm.

TABLE 2: Summary of the measurement results, comparing the use of a local scale bar for measurements that were taken via a photograph (data product-5) and a manual data-collecting process (data product-0).

Scale bar	Distance (measured)	Distance (model)	Error
Control point 5_point 7	1.81 m	1.81 m	1.11022e-15 m
Check point 1_point 2	2.51 m	2.6 m	9 cm
Check point 3_point 4	2.7 m	2.8 m	10 cm
Check point 5_point 6	2.2 m	2.1 m	10 cm
Check point 7_point 8	3.64 m	3.7 m	6 cm
Average			8.8 cm

A brief note should be given here on a limitation in terms of the field test that has been described and in the results that are presented in Table 2: the level of accuracy for the measurements in data product-5 was only assessed from the four points and only in two dimensions (replicating the manual measurements that were taken in data product-0). In contrast, the accuracy of data products-2 and 3 are assessed on a three-dimensional scale and without limits to the reference points (see the relevant point clouds in Figure 7 and Figure 8). To be able to properly assess the comparative accuracy of the use of a local scale bar, the relevant data product should include measurements taken in three dimensions (ie. x, y, and z).

Finally, Table 3 provides a summary of all of the data that was collected, presenting the time taken to collect the measurements and the level of

accuracy calculated for each data product. Accordingly, the table sorts the methods used into an order that is based on the time taken to collect the data (see Column 4 in Table 3), and based on the accuracy of the measurements (see Column 6 in Table 3). The experimental results that are presented in the table show that when collecting data with drones, completing the process using separate geo-referencing equipment takes significantly more time than does using built-in geo-referencing alone. Yet, when comparing the two methods of geo-referencing data to the measurements from the terrestrial scanner, the separate geo-referencing technology provides significantly more accurate data. At the same time, using a local scale bar in applying photogrammetry for data that is collected by drones can provide an alternative to geo-referenced data, as the results of the measurements that are taken in this field test show that the errors of margin differ from between 1.3 cm and 2.1 cm.

TABLE 3: Summary of the data collection times and accuracy levels for each data product.

Model number	Model name	Time	Place	Accuracy error	Place
0	Measuring wheel measurements and photographing	20 minutes	II	-	-
1	Terrestrial scanner	50 minutes	III	0 cm (globally geo-referenced)	-
2	Drone and 15mm RGB camera, with RTK GNSS geo-referencing	20 minutes	II	6.7 cm (globally geo-referenced)	I
3	Drone and 45mm RGB camera, with RTK GNSS geo-referencing	20 minutes	II	7.5 cm (globally geo-referenced)	II
4	Drone and 45mm RGB camera, with drone GNSS geo-referencing	5 minutes	I	481 cm (globally geo-referenced)	IV
5	Drone and 45mm RGB camera, with scale bar geo-referencing	5 minutes	I	8.8 cm (locally geo-referenced), 481 cm (globally geo-referenced)	III

CONCLUSIONS

As has been shown in the discussion in Section 1, whilst there is a growing body of research into new means of carrying out data collection and measurements at accident sites, that research is still ongoing and the methods being used are still under investigation. The larger research project to which this paper belongs is examining the potential for adopting photogrammetry via drone as a form of technology that is complementary to current practice. The results of the field test that are described here offer some support in that direction.

The results of the field test that have been described in the previous section provide specific data points on the accuracy of specific technological solutions that can be used in relation to data collection and taking measurements at scenes of accidents (corresponding to the five data products), as well as on the time taken to capture the relevant measurements when employing those forms of technology. As discussed in earlier sections, the motivations behind the study of the efficacy of photogrammetry via drone technology are to enhance accuracy, provide additional opportunities to process data, such as in terms of re-measuring the scene of an accident, provide additional viewpoints and, possibly, to reduce the time taken to complete the entire process. More specifically in the Estonian context, ongoing demographic changes, and therefore, changes to the available workforce, add a greater sense of urgency to the need to identify forms of technology that will fit in with these criteria. Considering the multi-dimensional nature of these requirements, however, the specific data points that result from the current field test cannot be taken alone when it comes to establishing the suitability or otherwise of the relevant forms of technology. Having said that, there are some inferences that seem reasonable to make based upon the data provided.

Firstly, so long as global geo-referencing is not required, the model that best balances accuracy and speed appears to be data product-5, which was considerably faster in terms of processing than all of the other viable methods (ie. data products-1, 2, and -3), with only marginal losses in terms of accuracy. Data product-4 took the same amount of time to process as data product-5, but was by far the least accurate, marking it

out as an unsuitable candidate for use in this field of operations, either in place of or complementary to existing practices. Addition to costs in terms of time, the Leica C10 ScanStation laser scanning system that was used to generate data product-1, as well as the RTK GNSS system that was used in data products-2 and 3, are significantly more expensive, as well as requiring additional training to deploy, than are the equipment and resources required for the local scale bar method that was employed to generate data product-5. Again, whilst not providing conclusive evidence that would satisfy the criteria needed to justify the uptake of drone technology, it seems reasonable to infer that there are at least some considerable advantages to the use of the local scale bar use, i.e. the possibility of being able to use photogrammetry for accident site measurements at a considerably lower cost than when geo-referencing the data.

That said, there are two significant limitations to this method that are worth recognising before further study is conducted. Firstly, over and above speed, time, and cost, geo-referenced measurements can add additional value when it comes to further analysis and investigation, e.g. via the production of metadata that can make possible the identification of wider accident patterns. The local scale bar method that was used to generate data product-5 would not allow such an option. Secondly, as briefly mentioned above, drone technology in general is subject to several use limitations, e.g. weather conditions, plus the physical features of the accident site and the site type, both of which are extremely significant when it comes to the possibility of being able to fly a drone in any specific case (Padua *et al,* 2020). (For further analysis of UAV use for photogrammetry within the context of Baltic weather, see also Suziedelyte Visochiene *et al,* 2016.) Moreover, as was the case in the field test described here, additional lighting is needed to produce high quality photos, and erecting such lighting at the accident site can add additional time (which was not measured here, but see John Hopkins University, 2018, p 57 for further discussion), which may significantly extend the time required for measurements to be taken and data collection to be completed.

Having noted these limitations on the available technology, however, the paper can put forward the opinion that the positive comparisons and inferences that have been noted above and which have been supported

by the field test that has also been described in this paper provide solid grounds for the further study of the suitability of the use of a local scale bar in relation to data collection and measurements at the scene of a traffic accident.

Contacts:

Jaanika Puusalu
Estonian Academy of Security Sciences,
Internal Security Institute
E-mail: jaanika.puusalu@sisekaitse.ee

Andres Mumma
Estonian Academy of Security Sciences,
Drones and Remote Sensing Centre
E-mail: andres.mumma@sisekaitse.ee

REFERENCES AND SOURCES

Bartoš, K., Pukanská, K., Repán, P., Kseńak, L. & Sabová, J. (2019). 'Modelling the Surface of Racing Vessel's Hull by Laser Scanning and Digital Photogrammetry'. *Remote Sensing, 11*(13), pp. 1526-1545.

Bengal, J. (2018). 'Drones Help Officials Investigate Auto Crashes but Raise Privacy Concerns', *State Legislature Magazine,* September/October. Available at: https://www.ncsl.org/research/transportation/drones-help-investigators-find-crash-causes.aspx (Accessed: 31 august 2020).

Blincoe, L. J., Miller, T. R., Zaloshnja, E., & Lawrence, B. A. (2015) *The economic and societal impact of motor vehicle crashes, 2010. (Revised) (Report No. DOT HS 812 013).* Available at: https://crashstats.nhtsa.dot.gov/Api/Public/ViewPublication/812013 (Accessed: 31 august 2020).

Cooper, S.D., Roy, D.P., Schaaf, C.B. & Paynter, I. (2017). 'Examination of the Potential of Terrestrial Laser Scanning and Structure-from-Motion Photogrammetry for Rapid Nondestructive Field Measurement of Grass Biomass'. *Remote Sensing, 9,* pp. 531-545.

Dukowitz, Z. (2020).' Drones in Accident Reconstruction: How Drones Are Helping Make Traffic Crash Site Assessments Faster, Safer, and More Accurate'. *UAV Coach,* 4 June 2020. Available at: https://uavcoach.com/drones-accident-reconstruction/ (Accessed: 20 September 2020).

Eyerman, J., Mooring, B., Catlow, M., Datta, S., & Akella, S. (2018) *Low-light collision scene reconstruction using unmanned aerial systems.* Accessible at: https://www.rti.org/publication/low-light-collision-scene-reconstruction-using-unmanned-aerial-systems (Accessed: 31 august 2020).

Eurostat (2019) Elanikkonna struktuur ja vananemine. Available at: https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Population_structure_and_ageing/et#Eakate_inimeste_osakaal_kasvab_j.C3.A4tkuvalt (Accessed: 23 September 2020).

Griffard, M. (2019). 'A Bias-Free Predictive Policing Tool?: An evaluation of the NYPD's Patternizr'. *Fordham Urban Law Journal,* 47 (1), pp. 43-83.

Guisado-Pintado, E., Jackson, D. W.T. & Rogers, D. (2019). '3D mapping efficacy of a drone and terrestrial laser scanner over a temperate beach-dune zone'. *Geomorphology*, 328, pp. 157-172.

Jurkofsky, D. (2015).'Accuracy of SUAS Photogrammetry for Use in Accident Scene Diagramming'. *SAE Int. J. Trans. Safety, 3* (2), pp. 136-152.

Kamnik, R., Perc, M.N. & Topolšek, D. (2019). 'Using the scanners and drones for comparison of point could accuracy at traffic accident analysis'. To be published at *Accident Analysis and Prevention.* [Preprint] Available at (by

request): https://www.researchgate.net/publication/337889744_Using_the_scanners_and_drone_for_comparison_of_point_cloud_accuracy_at_traffic_accident_analysis (Accessed: 12 June 2020)

Kersten, T.P., Mechelke, K., Lindstaedr, M. & Sternberg, H. (2008) 'Geometric Accuracy Investigation of the Latest Terrestrial Laser Scanning Systems', *FIG Working Week 2008,* Stockholm, Sweden 14-19 June 2008. Available at: https://www.researchgate.net/publication/253849299_Geometric_Accuracy_Investigations_of_the_Latest_Terrestrial_Laser_Scanning_Systems(Accessed: 31 august 2020).

Merriam-Webster. (2020) 'Drone'. Available at: https://www.merriam-webster.com/dictionary/drone?utm_campaign=sd&utm_medium=serp&utm_source=jsonld (Accessed: 25 august 2020)

Oguchi, T., Hayakawa, Y.S. & Wasklewicz, T. (2022). 'Chapter Seven - Data Sources'. *Developments in Earth Surface Processes,* 15, pp. 189-224.

Oniga, V.-E., Breaban, A.-I., Pfeifer, N. &Chirila, C. (2020). 'Determining the Suitable Number of Ground Control Points for UAS Images Georeferencing by Varying Number and Spatial Distribution'. *Remote Sensing, 12,* pp. 876-900.

Osman, M. R. & Tahar, K. R. (2016). '3D accident reconstruction using low-cost imaging technique'. *Advances in Engineering Software*, 100, pp. 231-237.

Pádua, L., Sousa, J., Vanko, J., Hruška, J., Adão, T. , Peres, E., Sousa, A. & Sousa, J. J. (2020). 'Digital Reconstitution of Road Traffic Accidents: A Flexible Methodology Relying on UAV Surveying and Complementary Strategies to Support Multiple Scenarios'. *International Journal of Environmental Research and Public Health*, 17, pp.1868-1892.

Pagounis, V., Tsakiri, M., Palaskas, S., Biza, B. & Zaloumi, E. (2006). '3D Laser Scanning for Road Safety and Accident Reconstruction'. *Shaping the Change, XXIII FIG Congress, Munich,* Germany, 8-13 October. Available at: https://fig.net/resources/proceedings/fig_proceedings/fig2006/papers/ts38/ts38_03_pagounis_etal_0475.pdf (Accessed: 31 august 2020).

Perez, J. A., Gonçalves, G.R., Galván Randgel, J.M., & Fuentes Ortega, P. (2019). 'Accuracy and effectiveness of orthophotos obtained from low cost UASs video imagery for traffic accident scenes documentation'. *Advances in Engineering Software*, 132, pp. 47-54.

Queensland Police (2019). 'QPS now using drone technology at traffic incidents'. *Queensland Police News, Queensland,* 10 October, Available at: https://mypolice.qld.gov.au/news/2019/10/10/qps-now-using-drone-technology-at-traffic-incidents/ (Accessed: 31 August 2020).

Rosell-Polo, J.R., Gregorio, E. & Llorens, J. (2019). 'Special Issue on "Terrestrial Laser Scanning": Editors' Notes'. *Senosors,* 19, pp. 4569-4576.

SAU - Urban Accident Analysis System. (2007) *SAU project: Guide of 'best practices' for the collection, processing and analysis of road accident data in urban zones.* Available at: https://www.uv.es/sau/eng/Results.wiki (Accessed: 31 August 2020).

Senquin, C. (2019). 'Drones shown to make traffic crash site assessments safer, faster and more accurate'. *Purdue University, Research Foundation News,* 16 January 2019, Available at: https://www.purdue.edu/newsroom/releases/2019/Q1/drones-shown-to-make-traffic-crash-site-assessments-safer,-faster-and-more-accurate.html (Accessed: 20 September 2020).

Shinar, D., Treat, J.R., & McDonald, S.T. (1983). 'The Validity of Police Reported Accident Data'. *Accident Analysis & Prevention,* 15 (3), pp. 175-191.

Statistics Estonia (2020a) Liiklusõnnetused 2019. Available at: https://www.stat.ee/34658 (Accessed: 17 April 2020)

Statistics Estonia (2020b) TS32: Sõidukid ja erasõidukid, 31. detsember. Available at: http://andmebaas.stat.ee/Index.aspx?lang=et&DataSetCode=TS32 (Accessed: 23 September 2020)

Su, S., Liu, W., Li, K., Yang, G., Feng, C., Ming, J., Liu, G., Liu, S. & Yin, Z. (2016). 'Developing an unmanned aerial vehicle-based rapid mapping system for traffic accident investigation'. *Australian Journal of Forensic Sciences, 48*(4), pp. 454-468.

Suziedelyte Visockiene, J., Puziene, R., Stanionis, A. & Tumeliene, E. (2106). 'Unmanned Aerial Vehicles for Photogrammetry: Analysis of Orthophoto Images over the Territory of Lithuania'. International Journal of Aerospace Engineering. Available at: https://www.hindawi.com/journals/ijae/2016/4141037/ (Accessed: 18 September 2020).

Tedinnick, R., Smith, S. & Ponto, K. (2019). 'A cost-benefit analysis of 3D scanning technology for crime scene investigation'. *Forensic Science international: Reports,* 1, pp. 1-12.

The John Hopkins University (2018) *Operational Evaluation of Unmanned Aircraft Systems from Crash scene reconstruction. Operational Evaluation Report. Version 1.0.* Available at: https://www.ncjrs.gov/pdffiles1/nij/grants/251628.pdf (Accessed: 31 August 2020).

The North Carolina Department of Transportation (2017) *Collison Scene Reconstruction & Investigation: Using Unmanned Aircraft Systems.* Available at: https://www.ncdot.gov/divisions/aviation/Documents/ncshp-uas-mapping-study.pdf (Accessed: 31 August 2020).

The Ministry of the Interior of Estonia (2020) *Siseturvalisuse arengukava 2020–2030 kavand.* Available at: https://www.siseministeerium.ee/et/STAK2030 (Accessed: 6 April 2020).

The Ministry of the Interior of Estonia (2019) *Siseturvalisuse arengukava 2020–2030 koostamise* ettepanek. VK nr 217. Available at: https://

www.valitsus.ee/sites/default/files/content-editors/arengukavad/stak_koostamise_ettepanek_09.2019.pdf (Accessed: 6 April 2020).

The Republic of Estonia Road Administration. (2020) Inimkannatanutega liiklusõnnetuste statistika. Available at: https://www.mnt.ee/et/ametist/statistika/inimkannatanutega-liiklusonnetuste-statistika (Accessed: 1 September 2020).

Yakar, M., Yilmaz, H.M. & Mutlouglu, O. (2014). Performance of Photogrammetric and Terrestrial Laser Scanning´Methods in Volume Computing of Excavtion and Filling Areas'. *Arabian Journal for Science and Engineering,* 39, pp. 387–394.

Zhuo, X., Koch, K., Kurz, F., Fraundorfer, F. & Reinartz, P. (2017). 'Automatic UAV Image Geo-Registration by Matching UAV Images to Georeferenced Image Data'. *Remote Sensing, 9,* pp. 376-402.

Šašak, J., Gallay, M., Kańuk, J., Hofierka, J. & Minár, J. (2019). 'Combined Use of Terrestrial Laser Scanning and UAV Photogrammetry in Mapping Alpine Terrain'. *Remote Sensing,* 11, pp. 2154-2179.

DEVELOPING THE SITUATIONAL AWARENESS OF INCIDENT COMMANDERS: EVALUATING A TRAINING PROGRAMME USING A VIRTUAL SIMULATION

Stella Polikarpus (corresponding author), MA
Estonian Academy of Security Sciences
Studies in Tallinn University

Tobias Ley, PhD
Professor
Tallinn University

Katrin Poom-Valickis, PhD
Professor
Tallinn University

Keywords: situational awareness (SA), rescue incident commanders (ICs), virtual simulation, The effective command behavioural marking framework (EC), the Kirkpatrick model

ABSTRACT

Life, property, and the effectiveness of efforts involved in saving the environment depend upon the situational awareness of incident commanders. However, so far, the impact of situational awareness training for working rescue incident commanders has not been studied in Estonia. This study aims to evaluate situational awareness training that has currently been implemented as an overall part of the dynamic decision-making model for all rescue incident commanders in Estonia. The new training curriculum, plus training materials and methods, were developed for situational awareness training using the virtual reality software, XVR On-Scene, and the Moodle e-learning environment. Assessors were trained and certified to apply the effective command behavioural marking framework to measure situational awareness. The Kirkpatrick training programme evaluation model was adopted to measure the SA training outcomes. Based on the Kirkpatrick model, Level 1 trainee reactions indicated that Estonian rescue incident commanders were able to accept a new approach to their decision-making training as a purposeful and engaging way of completing their attestation. Their basic psychological needs were supported during the training process, and participants achieved higher-than-threshold results in all SA levels, as is shown in Level 2 of the Kirkpatrick model. Training programme evaluation model Level 3 behaviour, and Level 4 results, need to be further studied. Suggestions have been provided in improve the virtual simulation-based training and assessment of situational awareness.

INTRODUCTION

Rescue incident commanders (henceforth referred to as ICs) are first responders. They need to make independent and effective decisions in time-critical and life-threatening situations (Allas *et al,* 2018). The fact has been highlighted in several studies that decision-making experiences which ICs gain from their work are limited, and the consequences of dynamic decision-making can be life-threatening (Cohen-Hatton, Butler and Honey, 2015; Lamb, Boosman, and Davies, 2015). Endsley stated that '*Situational awareness is knowing what is going on around you*' (Endsley, 2000). The situational awareness of ICs (with situational awareness henceforth being referred to as 'SA') can determine the chances of survival both of rescuers and those they are rescuing, as well as the extent of property and environmental damage. An SA has three levels: perception, comprehension, and projection (Endsley, 2000). To be able to train and assess SA levels is a complex task. ICs with good levels of SA can produce safer decisions if they have previously practiced dynamic decision-making while using virtual simulations (Williams-Bell *et al,* 2015). To train and assess SA, realistic rescue events can be represented using various virtual simulations (Polikarpus, Bøhm, and Ley, 2019).

The Estonian Rescue Board, together with the Estonian Academy of Security Sciences (henceforth referred to as the EASS), has developed and implemented working SA training and assessment for ICs to ensure better decision-making. All tactical level incident commanders in Estonia take part in the training programme. The aim of the study is to evaluate the situational awareness training as part of the dynamic decision-making training and assessment programme that is being implemented for rescue incident commanders. The training and assessment programme's evaluation work is carried out based on Kirkpatrick's well-known and long-used four level model which consists of levels covering trainee reactions, learning, behaviour, and results (Kirkpatrick and Kirkpatrick, 2006, p. 21). The same model was recently used to evaluate a simulator-based ambulance driver training day (Prohn and Herbig, 2020), and therefore is well suited to the needs of the current study.

Until 2016, the annual assessment of working ICs in Estonia was carried out by using a multiple-choice question format. Dynamic decision-making skills and SA as part of this was not something that was provided for in training and neither was it measured. During 2016, the student-centred training programme was developed with the aim of training and assessing IC decision-making skills. As part of the new training programme, the SPAR decision-making model (which stands for Situational awareness, Plan, Action, Review) was introduced (Launder and Perry, 2014). The SPAR dynamic decision-making model helped to train and assess SA using virtual simulation.

Virtual simulation-based training is considered to be a flexible, student-centred way of training internal security staff for joint response actions to accidents (Põder, Savimaa, and Link, 2015). Training and assessment of and for dynamic decision-making skills could be carried out using virtual simulations (Lamb, Boosman, and Davies, 2015). Endsley, the author of the SA construct, advises on the use of simulations to measure SA levels (Endsley, 1995a). At the same time, not enough empirical studies have been carried out that show how the use of virtual simulations improves learning (Girard, Ecalle and Magnan, 2013). There is lack of guidance regarding how to integrate a virtual simulation-based SA training systematically into IC training.

Effective use of virtual simulations to improve SA training requires it to be integrated systematically into an approach to training and assessment. Therefore, our research question is how can situational awareness training be provided to ensure different levels of situational awareness as part of dynamic decision-making training using virtual simulations? In order to address this question, we first give an overview of the development of the training programme. Then, we evaluate outcomes of the programme that used the e-learning course, the XVR On-Scene virtual simulation software, and the effective command behavioural marking framework to be able to train and assess SA as part of the dynamic decision-making process.

1. SITUATIONAL AWARENESS

Models are required to be able to carry out decision-making training. '*Specific kinds of expertise requires specific mental models that are assumed to develop over time and with experience*' (Chermack, 2003, p. 416). Until now in Estonian Rescue Board incident command documentation, use has been made of the decision-making model that is known as 'Observe, Decide, Command and Control' (in Estonian, this is LOKK: *Luure, Otsustamine, Käsklemine, Kontroll*). There are several other decision-making models that are available, such as, for example, OODA ('Observe, Orientate, Decide, and Act'), or DOODA ('Dynamic OODA'), or FORDEC ('Facts, Options, Risks (or benefits), Decide, Execute, and Check'), or FADCM ('Factfinding, Analysis, Decision-making, Communication, and Monitoring') (Groenendaal, 2015, pp. 58–59). However, none of them includes SA. Therefore, as part of the new training programme for working ICs in Estonia, the selection was made of SPAR ('Situational awareness, Plan, Action, Review') (Launder and Perry, 2014) to be used for training and assessment in terms of SA.

The creators of the SPAR model identified five key dynamic decision-making behavioural elements: 1) Situational awareness; 2) Decisions; 3) Plan; 4) Action; 5) Review. They claim that all these behaviours are associated with effective command competence in urban fire settings (Launder and Perry, 2014). The effective command behavioural marking framework assesses all of these behaviours (Lamb *et al,* 2020).

Endsley defines SA as: '*the perception of the elements in the environment within a volume of time and space, comprehension of their meaning, and the projection of their status in the near future*' (Endsley, 1995a). The measurement of SA depends upon the circumstances, time, place, and person (Endsley, 1995b). In this article, we focus only on first behaviour in the SPAR dynamic decision-making model in regard to SA. The SA levels are as follows: Level 1 covering information collection by ECs, or Endsley names perception; Level 2 covering comprehension in ECs; and Level 3 covering evaluation by ECs or prediction (Endsley, 2000).

Situational awareness as part of dynamic decision-making training is important for all first responders, as they need to make decisions in highly challenging environments and high stakes situations under considerable time pressure (Cohen-Hatton, Butler, and Honey, 2015). In such situations, it is not only the responders themselves who are at risk, but also members of the public, plus property and the environment. SA is indispensable in the decision-making process (Endsley, 1995b). Unfortunately, dynamic rescue incidents always bring with them high levels of risk for the participants, so they cannot be systematically used to train SA.

2. RESCUE INCIDENT COMMANDER TRAINING IN ESTONIA

The SA construct was not used in Estonia rescue service until the year 2016. Tactical level rescue ICs in Estonia are referred to as 'rescue unit leaders' and 'rescue leaders'. There are vocational occupation standards for both of the jobs, having been developed in 2013 and updated in 2018 (Kutsekoda, 2020). In 2018, there were 409 ICs working in shifts that provided cover twenty-fours hours a day and seven days a week (Tammik, 2019). All tactical level rescue ICs in Estonia are male.

Before 2016, the command knowledge of ICs in Estonia was assessed every year using computer-based multiple answer tests. For IC trainers in the EASS, it seemed that this form of attestation was not especially motivating or engaging for commanders. Based on research, we know that if the psychological needs of trainees are fulfilled (covering areas, such as autonomy, competence, and relatedness) then the trainee in question will feel motivated and engaged (Ryan and Deci, 2000), with higher motivation and engagement levels supporting the learning process (Knight, 2016). Therefore, the new training programme for practising and measuring dynamic decision-making, which includes SA, was developed based on three principles. Each rescue IC in Estonia should have an opportunity to take command at an incident within a virtual simulation. Virtual simulation can be used to create time pressure and high stakes situations for ICs, providing engaging learning experiences (Polikarpus, Bøhm and Ley, 2019). To implement, this the widely used XVR On-Scene virtual reality software was selected (henceforth referred to as XVR OS) (XVR Simulation, 2020).

Secondly, the decision-making skills of each rescue IC should be assessed based on a virtually simulated incident command. In order to be able to implement this, the effective command behavioural marking framework was selected as an assessment tool (Effective Command, 2020). The framework was developed to align with the UK National Fire Service competency role maps (Fire Central Programme Office, 2020). This is used in several countries in Europe, such as, for example, the UK, Portugal, France, and Italy (Lamb *et al,* 2020).

Thirdly, the e-learning platform for all ICs in Estonia should be applied in order to bring together theory, documentation, and computer-based testing of knowledge. To be able to implement this, Hitsa Moodle was selected (Hariduse Infotehnoloogia SA, 2020).

Based on three earlier-named principles, the student-centred training programme known by the name 'Training and Assessment Day' (henceforth referred to as TAD) was developed in the year 2016. The aim of TAD is to evaluate whether the command competence of working ICs was at the level required by a 'Rescue Unit Leader' in terms of the occupational qualification standard (Polikarpus, 2016). This is targeted towards a tactical level working IC across the entirety of Estonia. We hereby explain the design steps used in TAD.

1) Mapping the EC with the Level 5 vocational occupation standard required for a rescue unit leader. From the mapping perspective, it was concluded that the EC measures only those commanding competences that are based on the SPAR decision-making model.

2) EC licences were purchased for the web-based tool and for assessor training. The EC assessment tool divides SPAR into eight sections, with SA having three subsections: 1) information gathering; 2) comprehension; and 3) evaluation. Every section has nine criteria, which are assessed on a sliding scale of five points, from dark red to dark green. The yellow in the middle refers to the threshold. The EC tool scale is positioned on yellow (3), in the middle of the five-point scale (see Figure 1). The dark red (1) and light red (2) are seen as providing an under-achieving learning outcome, and the light green (4) and dark green (5) are seen as providing an over-achieving learning outcome (Effective Command, 2020).

Assessor training was carried out first in English and later in Estonian. To be able to start to work as assessor, it was obligatory to take part of XVR OS user training together with work experience from incident command situations. All of the assessors are certified and re-certified by the EC organisation on an annual bases (Effective Command, 2020). The certification process is required to ensure competence in external evaluations for assessors, and it also ensures the validity of the assessment instrument and the reliability of the assessments themselves.

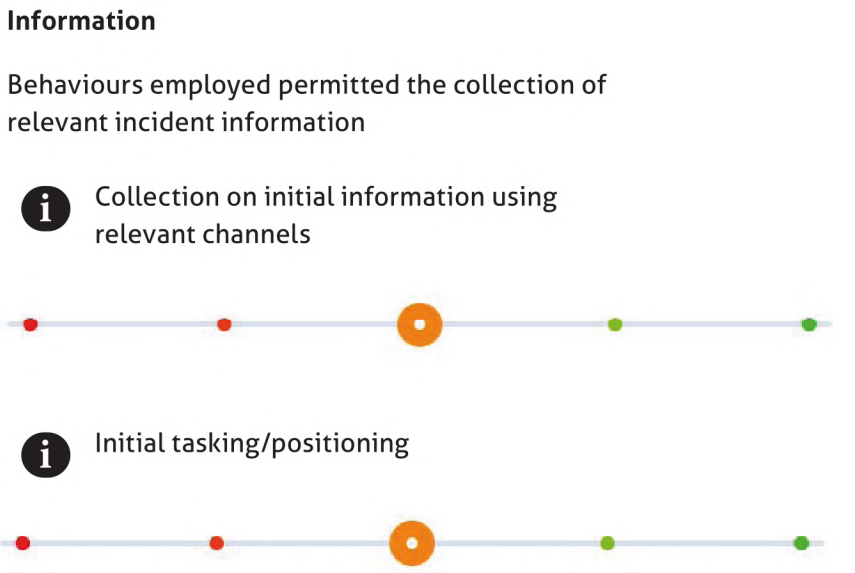


FIGURE 1: The scale used in the framework assessment tool for effective command behavioural markers.

3) Assessment scenarios are composed on the XVR OS platform. It is a challenging and time-consuming task. Each year, twelve new scenarios need to be created. In EASS-implemented pair-authoring, a seven step procedure is required to build assessment scenarios. First, the scenario map is presented to start the procedure of building and each scenario are drawn up in the form of the XVR OS fail and scenario user manual. The procedure ensures that the XVR OS fail and storyline comply with the EC framework and that the virtual simulation is as authentic as possible.

4) The TAD training curriculum was written out (Polikarpus, 2016). The curriculum was coordinated with the Estonian Rescue Board and the EASS additional training centre.

We now explain the TAD implementation. First TAD was completed on 4 April 2016. Last TAD included in the study was carried out on 21 February 2020.

1) The TAD started with a ninety minute lecture in which an SA construct was discussed with a group of four trainees.

2) The training scenario lasted for ninety minutes. Joystick exercises and full dynamic play of the training scenario was carried out in the form of one-to-one training.[1]

3) The formal assessment was carried out over the course of between 90–120 minutes. Two certified assessors handled the SA assessments in three phases: a) a dynamic assessment phase in which one assessor took on the roll of a technical instructor who was manipulating the XVR OS software. The other provided voices for avatars and checked that important changes in the situation were played out based on the scenario user manual. In this phase, the ICs review of the situation is tested to make sure that the IC in question can update their SA throughout the incident response. The virtual simulation allows the IC to execute their incident response plan. The dynamic phase ends with the IC's higher level commander arriving on scene. The trainee provides an overview of the situation to an assessor so that their SA can be checked. Phase b) involves a feed-forward conversation between the trainee and their assessors. The aim of the reflective dialogue is to find out how the IC themselves evaluate their SA in the response phase. Phase c) is when the EC certificate is filled out by both assessors. This is submitted to the EC database after the assessors have jointly marked each assessment criteria.

4) Formal assessment results are sent to the Estonian Rescue Board. There are three summative assessment outcomes that are coded by colour: green means excellent, yellow means threshold, and red means under the threshold. An IC who achieves a green summative assessment result is assessed again after a space of three years, while a yellow result will mean a reassessment after two years, and a red result means a repeat assessment at a point between just six months later and a year.

After piloting the TAD in spring 2016, trainee feedback and learning was analysed and the following changes were made to the programme:

1) The TAD curriculum was changed from six contact classes to a course lasting 52 hours, because it became clear that more theoretical input is needed for any implementation of SPAR and SA. There were a total

[1] The training scenario being used is fully described in article: 'A training incident commander's situational awareness – a discussion of how simulation software facilitates learning' (Polikarpus, Bøhm, and Ley, 2019).

of eight threshold-level-phrased learning outcomes for each EC section (Polikarpus, 2016). Three learning outcomes were related to SA (Polikarpus, Bøhm and Ley, 2019).

2) An e-learning course was developed to support preparation for TAD, utilising Hitsa Moodle. The e-learning materials were designed for 46 hours of work. The e-learning course is targeted at rescue unit leaders. However, it is suggested that rescue leaders also take part.

3) The re-assessment curriculum for ICs was developed for ICs who had already been assessed once. It covers four academic hours and has the same SA learning outcomes and e-learning course (Polikarpus, 2017).

Since 2019, the six hours curriculum has been stopped because all of the ICs in Estonia had already completed it. Only the re-assessment curriculum is now being used in EASS for the attestation of Estonian tactical level ICs.

To be able to evaluate SA at different levels of training as part of the implemented dynamic decision-making for rescue incident commanders during TAD, we conducted the study based on the Kirkpatrick training programme evaluation model.

3. METHODOLOGY AND DATA COLLECTION

To be able to evaluate the effectiveness of TAD, Kirkpatrick's well-used training programme evaluation model was used, which has four levels: Level 1 covers trainee reactions; Level 2 covers learning; Level 3 covers behaviour; and Level 4 covers results (Kirkpatrick and Kirkpatrick, 2006, p. 21). A literature review regarding the implementation of the Kirkpatrick model claims it to be suitable for the evaluation of any training programme from two perspectives: organisation when implementing training; and those members of staff who will participate (Smidt *et al,* 2009). We report the views of TAD participants in the years 2016–2020 and our sample covers entirely tactical-level rescue ICs in Estonia.

The Level 1 trainee reactions can, typically, be measured by allowing them to complete a post-training evaluation to discover their impressions of the programme (Smidt *et al,* 2009). To measure trainee reactions, we asked the following questions, starting with: how purposeful and challenging is SA training during TAD when SPAR and virtual simulation is used? An additional question covered: how engaging and motivating is TAD for ICs?

To evaluate trainee reactions to TAD, use was made of survey results covering anonymous training feedback from 2016–2020. There are twelve predefined multiple-choice questions available, with the option of being able to add personal comments to each question (see Table 1). This was sent to the official e-mail addresses of ICs after they had participated in TAD. Altogether 196 responses were received via LimeSurvey. Unfortunately, not all ICs responded. After the full sample of ICs in Estonia had at least one opportunity to participate in TAD, the study bases for the master theses were undertaken (Tammik, 2019). The study worked out the engagement and motivation levels for trainees during TAD. The research proves that learning is supported by ensuring high engagement levels with trainees, along with fulfilling their basic psychological needs (Ryan and Deci, 2017). Therefore, in this paper, the study is referred to as the engagement and motivation study (see Table 1). The sample basis for the study was a total of 393 ICs, all of whom had participated in TAD at a point between 2016–2018. The anonymous self-reported web-based

Estonian language survey via LimeSurvey was sent to ICs via their official work email addresses. The survey had various parts that needed to be completed and which evaluated motivation, engagement, the purposefulness of TAD, and the difficulty level of the scenarios (see Table 1). No comments could be added to the statements. A total of 224 respondents correctly filled out their responses and all of these were collected. Not all data from the study is presented in this paper. The study as a whole can be found in the master theses (Tammik, 2019).

The second level of the Kirkpatrick model is learning (Kirkpatrick and Kirkpatrick, 2006). On that level, measurements that are used to quantify learning include knowledge tests or skills demonstrations in the form of roll-plays (Smidt *et al,* 2009). We asked whether ICs in Estonia where able to learn about SA at different levels during TAD.

Evidence that ICs have indeed learned about SA were collected from two sources: EC formal assessment results and e-learning course test results (see Table 1). Formal assessment results were downloaded on 28 February 2020 from the EC database. There were altogether 533 formal assessment certificates in the dataset from between January 2017 and February 2020. The reason for such a high number of such record in the EC is that several commanders had been assessed twice. Formal assessments included (in Table 1) a total of 305 one-off formal SA assessment results and 114 that were assessed twice. Formal assessment results from 2016 were not included in the study. It should be remembered that EC measures are included in coloured scoring for all five of the key-behaviours of dynamic decision-making. The summation assessment outcome colour takes into account all eight parts of the assessment. However, in the current study, only the first three parts of the EC are reported upon. Formal assessment SA levels in EC are measured with nine assessment criteria on the five-point scale (see Figure 1, above). If five points (using the dark green colour) are marked out in each criterion, this means that the assessment results in a straightforward score of one hundred points on that level. If one point (in the dark red colour) is marked out in each criterion, a total of twenty points are still awarded in the overall assessment result for that SA level. Yellow, in the middle of the scale, is a threshold (Figure 1). If all of the criteria are left unmoved, a total of sixty points are calculated for the overall score. The 'excellent' SA level starts from a score of seventy points.

TABLE 1: Kirkpatrick model levels and the measurement instruments that were used.

Kirkpatrick evaluation levels	Measurement instrument	Data collection	Example statements or questions
Level 1: reactions	The engagement and motivation study based on self-determination theory. 224 respondents (Tammik, 2019)	Anonymous survey via LimeSurvey in year 2019. Parts of the used survey: 1. Autonomy need: measured with 6 statements in scale 1–7. Adopted from (Williams and Deci, 1996); 2. Competence need measured with 6 statements in scale 1–7. Adopted from (Jang, Reeve and Deci, 2010). 3. Relatedness need measured with 4 statements including 2 reversed ones in scale 1–7. Adopted from (Chen et al., 2015) 4. Engagement during TAD was measured with 12 statements, including 3 reversed ones in scale 1–7. Adopted from (Knight, 2016, p. 147)	1. "I felt assessors gave me choices" "I felt during the assessment that assessors understand me." 2. Choose on the scale to fit: (1) "TAD was an incomplete learning experience" and (7) "TAD was a perfect learning experience." 3. "I felt assessors were friendly" or reversed statement "I felt my communication with assessors was superficial." 4. "I paid attention during TAD" and reversed statement "I felt often disappointed during TAD"
	TAD feedback survey 196 respondents	Anonymous survey via LimeSurvey in years 2016–2020. There were 12 predefined answers questions with the possibility to add comments to each question.	"On what level you were engaged while responding to the incident in the virtual simulation?" "Did assessors' competence meet your expectations?"
Level 2: learning	533 EC assessment results	EC framework based formal assessment results from January 2017 – February 2020. Each SA level is scored from 20 to 100.	533 certificates were downloaded from the EC database. (28.02.2020.)
	Moodle situational awareness self-check test 672 completed test attempts	6 multiple choice questions in the SA self-checking knowledge test on Hitsa Moodle platform. Correct answer gave one point per question. All questions had four choices.	See Table 4 below for questions asked in the test. A number of correct answers for question 1 to 4 and 6 were three. Question nr 5 had one correct answer.

Level 3: behaviour	114 EC assessment results	Two times TAD participants formal assessment results. See above in this table.	See above in this table.
	TAD feedback survey 196 respondents	See above in this table.	"On what extent the response to the incident using virtual simulation developed your commanding competences?"
Level 4: TAD results were not analysed based on Kirkpatrick			

SA self-checking test results were downloaded from the Hitsa Moodle platform on 30 April 2020 (Table 1). One trainee could do the test as many times as they liked without a time limit being imposed. There were a total of 672 completed test attempts.

The Level 3 behaviour in the Kirkpatrick model measures trainee ability in the use of newly learned knowledge or skills in the workplace, and Level 4 results evaluates the overall process, including any financial or moral impact of training (Smidt *et al,* 2009). As stated in the introduction, assessing SA is a complex task. Due to this, it is very difficult to make any claims on Levels 3 and 4. Nonetheless we did ask whether TAD served to develop the command competences of ICs, and whether there was a significant change between two different SA level assessments.

We used a total of 114 formal IC assessments from between 2017–2020 for those ICs who had participated twice in TAD so that we could measure any potential behavioural change. The SA level means that the results from two separate assessments were compared. In the TAD feedback survey, the question was asked regarding competences development (see Table 1). This allowed trainees to subjectively report TAD effects on the behavioural level. The Kirkpatrick Level 4 results which measure overall training impact, including financial or moral impact, are outside the scope of this study. Table 1 presents the measurement instruments and datasets that were used for the TAD evaluation, based to the Kirkpatrick training evaluation model.

When it came to handling the data, descriptive statistical analyses were carried out using Microsoft Excel. Variables were described in terms of percentages or by the usual means and standard deviations. Formal SA assessment results were analysed using a single-factor ANOVA test, while for any *post hoc* testing the paired T-test was used.

4. RESULTS

Based on the Kirkpatrick model, when it came to evaluating trainee reactions to TAD, we asked how purposeful and challenging was SA training during TAD when SPAR and virtual simulation is being used.

IC reactions to TAD clearly indicate that 90% of trainees see the new form of attestation as being a purposeful and positive change (see Figure 2), while 97% saw the e-learning course as being useful. Unfortunately, no research has been carried out in regard to how purposeful ICs thought the computer-based multiple-choice tests would be for their command competence attestation. Altogether, a total of 202 individuals (or 90%) evaluated the use of virtual simulations as being purposeful or rather purposeful (see Figure 2). The purposefulness of using SPAR differed by only one individual, resulting in a total score of 203 individuals or 91%. Only four commanders did not consider the virtual simulation to be a

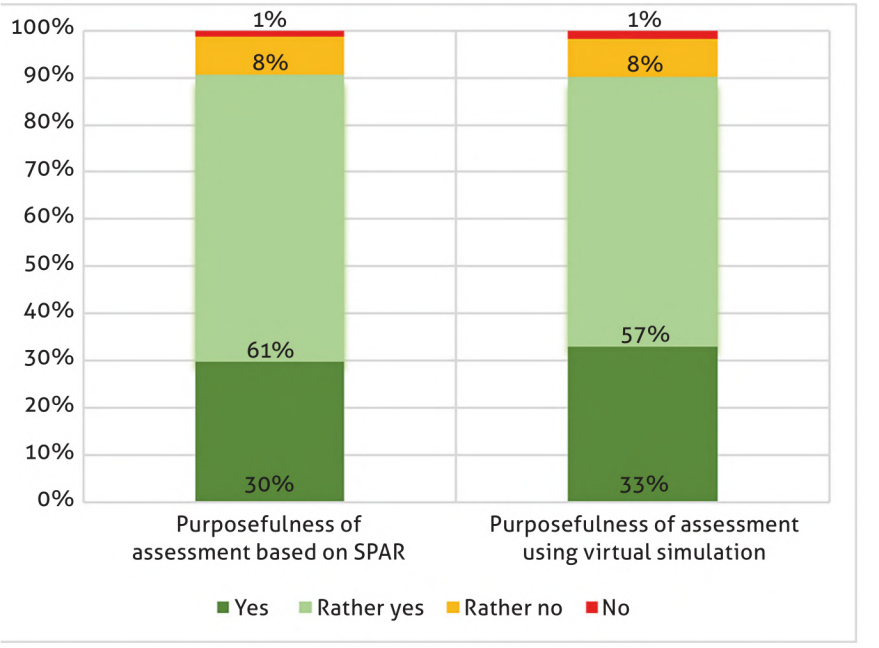


FIGURE 2: The purposefulness of the assessment method (self-reported; N = 224).

purposeful environment in which to carry out assessments, and three did not find the SPAR to be useful for assessments. In the TAD feedback survey, one IC commented on the purposefulness of the test: '*There is the possibility of being able to experience in a very short time various incidents in the simulation which could develop much more than just theory alone instead of simply providing a stock range of exercises. At the same time, any potential weak spots can be uncovered which require further development', while others stated: 'It was quite close to real life'.*

From 2017 onwards, an extra question was included in feedback survey regarding the e-learning course in Moodle. Only those ICs who had first indicated that they had been on the course and had been questioned about the usefulness of that course were asked the new question (N = 85). The e-learning course was stated to have been very useful a total of twice 39 times (46%) out of a total of 85 answers, and rather useful 43 times (51%). One person (1%) said it was rather useless, and two (2%) said it was completely useless.

If we looked at the reactions of other trainees to TAD using feedback survey responses (N = 196), it was encouraging to see that 92% (180) indicated that they did receive feedback from the assessors in regard to their SA. Even so, a total of 7% (fourteen) were not sure they had received any feedback about their SA, and two (1%) said they did not get any feedback at all from their assessors. Comments on the feedback that was provided included the following responses: '*A discussion following the dynamic phase of the incident response helped to find bottlenecks, and I received suggestions which would be useful in my own future development*'. Furthermore, 76% (149) of trained ICs indicated that the competence levels of the assessors fully met their expectations during TAD, and 21% (41) said it 'rather' did. Only the expectations of four individuals in regard to the competence levels of their assessors were classed as rather not having been met (2%), and two stated that the assessors did not at all meet their expectations.

In addition, Estonian ICs found a degree of challenge when it came to solving the virtual simulation-based scenarios. The self-reported TAD participants (N = 224) indicated on a scale of 1–7 that the response to the incident in the virtual simulation (M = 4.79; SD = 0.98) was slightly more challenging for ICs than were the scenarios for the incidents (M = 4.70;

SD = 0.97). In the TAD feedback survey (N = 196) half of the participants (53%; 104) said that the difficulty levels in the scenarios in the virtual simulation suited them, and 65 (33%) reported that it was rather difficult for them. It was commented upon that the virtual simulation made it somewhat challenging to gather information.

A second question we asked to be able to evaluate trainee reactions to TAD was how engaging and motivating the TAD was for the ICs.

Based on the engagement and motivation study, ICs found TAD to be engaging (M = 5.43 out of seven), and their psychological basic needs (autonomy needs of M = 5.77; competence M = 6.03; and relatedness M = 6.16, all out of seven) were well met (see Table 2). This means that their study-motivation levels were high during TAD. The engagement and motivation study that was used in the Survey 4 sections could be marked on a scale of 1–7. Firstly, an average was calculated for each participant's answers in every part of the survey. The overall mean and standard deviation for engagement and psychological needs is presented in Table 2.

TABLE 2: Engagement levels and psychological needs during TAD.

Part in study	Self-reported means (N=224)	Standard Deviation
Engagement	5,43	0,78
Autonomy need	5,77	1,13
Competence need	6,03	0,91
Relatedness need	6,16	0,99

We could conclude from Table 2 that all three psychological needs (autonomy, competence, and relatedness) are well met during TAD. The TAD feedback survey conforms well with this conclusion (N = 196). In regard to the question: '*On what level were you engaged while responding to the incident in the virtual simulation?*', a total of 148 participants (76%) responded with the following: '*I was fully engaged while responding to the incident*'. The answer was: '*I was partially engaged while responding to the incident*', was given a total of 44 times (22%), and the answer: '*I was not at all engaged while responding to the incident*' was ticked only by four persons (2%).

From the reactions of trainees, it could be concluded that the new training curriculum has been accepted very well by working ICs in Estonia. Trainees feel that their basic psychological needs (autonomy, competence, and relatedness) are being met during TAD. They showed positive reactions towards the new training programme, including e-learning and trainer competence and feedback received following their SA. The new training methods and tools being used for SA training were engaging for them.

Based on the Kirkpatrick model to evaluate trainee learning, we asked whether ICs in Estonia were able to learn about SA at different levels during TAD? To answer this, we analysed the formal assessment and the e-learning course self-check test results.

We wanted to evaluate whether all three SA levels are successfully being taught during TAD. Therefore, we have reported on the mean SA level assessment results in Table 3. Means and standard deviations were calculated for all ICs in Estonia, taking their last assessment result into account (the second column in Table 3).

TABLE 3: Average scores for situational awareness levels in rescue incident commanders.

Endsley SA levels	**All ICs last assessment mean and SD (N=419)**	**ICs assed once mean and SD (N=305)**	**ICs assessed twice mean and SD (N=114)**	
			First time	Second time
SA level 1: perception	68,50 (8,04)	69,39 (8,27)	67,78 (9,32)	66,11 (6,88)
SA level 2: comprehension	67,60 (8,38)	68,56 (8,61)	65,24 (10,72)	65,02 (7,13)
SA level 3: prediction	65,74 (8,98)	66,61 (9,39)	62,40 (10,60)	63,40 (7,32)

Firstly, we asked whether the assessment scores were valid indicators to allow a claim to be made that ICs have been taught in all of the SA levels. Based on learning outcomes in the SA levels and on previous IC training, we hypothesised that ICs with SA-level comprehension are better at collecting together the required information (at SA Level 1) than they

were in predicting the situation (SA Level 3). In Table 3, we can see that the average score for SA Level 1 is 68.50, while the SA Level 2 average is 0.9 oints lower, and the SA Level 3 average is 1.86 points lower than the SA Level 2. SA levels 1 and 3 differ from each other by a total of 2.76 points. As well as this, a growth of SD could be observed. Thanks to the average results being ascertained, the variety of gaps between the different SA levels could be seen in the expected order. To be able to find out whether the differences were significantly important, an ANOVA test was carried out in Excel. The results of a single-factor ANOVA test on the most recent assessment of all Estonian ICs (N = 419) indicated that there is a statistically significant difference between the averages for different SA levels ($F = 11.54$, $p < 0.001$). Post hoc paired t-test results fell between SA levels 1 and 2: $t = 3.02$; $p < 0.003$; SA levels 2 and 3: $t = 6.90$ $p < 0.001$; and SA levels 1 and 3: $t = 8.58$; $p < 0.001$. ANOVA and post hoc tests confirmed that there is a statistically significant difference between the different SA levels. Analyses of formal assessment results showed that EC formal assessments are valid when it comes to measuring all three SA levels.

Additionally, we asked how good an SA level did ICs in Estonia have according to their formal assessment results. Earlier, under data collection conditions, the coloured scoring in the EC framework was explained. Compared to the threshold in the summative assessment results, all three means for SA levels are on the threshold. None of the SA level means are at a level that could be considered excellent in the EC framework (seventy points). Because all three SA level means exceeded the threshold of sixty points, we can conclude that training for three SA levels is being provided during TAD at least at a level that provides a reasonable learning outcome. Previous training for ICs and the use of the decision-making *LOKK* model which was used in incident command guidelines could explain why there are significant differences between the scores being achieved for SA levels 1 and 3. For example, until 2016, a dynamic risk assessment was not supplied as part of the training programme. Furthermore, a dynamic risk assessment at an incident plays an important role in predicting the development of the situation.

To be able to measure theoretical knowledge in relation to the SA construct, the Moodle test results were used (Table 4). The test-taking times for trainees varied from just a minute to more than a year. Out

of 672 test results, 620 attempts were made which took less than fifteen minutes, while 484 took less than five minutes, and 248 less than three minutes. Self-checking test attempts showed that 205 trainees took the test just once and 164 took it more than once in the years 2016–2020. The average score for one-time test-takers out of the six-point multiple-choice test was 5.53. Trainees who have taken the test several times have done so between two and thirteen times. The maximum score had been achieved 218 times. After taking the test, trainees could see their overall rating and their correct answers for each question. There was no threshold for the test. The minimum score for one-time test-takers (N = 205) was 2.62, and test-takers who took part in the test several times made 467 attempts with a minimum score of 2.29. From the test attempts that have been logged, we argue that those ICs who got lower scores tended to retake the test. This highlights the importance of feedback in the learning process.

In Table 4, all the average and standard deviations for each question can be seen, complete with overall test results. The question: '*When you start to construct your SA*', had the lowest mean (M = 0.763). This is a disputable question in the test because, before the SPAR model was implemented, ICs were trained to carry out a 360 degree reconnaissance as part of the *LOKK* decision-making model (see Chapter 1). However, in the test scoring that answer did not provide any points because the entire SA construct was associated purely with 360 degree reconnaissance. The SA construct is more than simply carrying out a 360 degree reconnaissance, and this was the reason that the start of the SA was not associated with carrying out a 360 degree reconnaissance alone.

From the self-check tests and formal assessments, we were able to conclude that TAD has helped not only in terms of learning the SA theoretical concept but has also aided in the implementation of all SA levels during virtual simulation-based assessments.

As stated previously, evaluating the TAD in relation to the Kirkpatrick levels 3 and 4 is rather difficult, and TAD results for participants could not be measured because the SA levels are challenging if not impossible when it comes to measuring them in the real life work of ICs. However, based on the Kirkpatrick model in terms of evaluating trainee behaviour, we asked whether TAD had served to develop IC command competences,

TABLE 4: Knowledge test results for self-checking one's situational awareness.

Questions in the SA self-checking knowledge test	All attempts Mean and SD (N= 672)	Mean one-time test-takers (SD) (n = 205)	Max	Min
1. When you start to construct your SA?	0,763 (0,281)	0,743 (0,288)	1	0
2. When you start your shift what you do for your SA?	0,936 (0,164)	0,942 (0,150)	1	0
3. What are the levels of SA?	0,953 (0,153)	0,968 (0,119)	1	0
4.From whom IC can ask information?	0,915 (0,164)	0,908 (0,159)	1	0,33
5. What needs to be done if you have received the information you do not understand?	0,969 (0,174)	0,990 (0,099)	1	0
6. Why is it important to predict the situation development?	0,968 (0,118)	0,976 (0,098)	1	0

and was there a significant change between the assessments of SA levels for two-times takers?

TAD has served to develop IC command competences. This can be seen in the feedback survey (N = 196) with a figure of 95 (48%) of TAD participants indicating that they felt training helped to develop their command competences enough so that they were able to reach better decisions at work. Almost the same amount of commanders – 93 (47%) – ticked the box to say that TAD had 'rather' developed their command competences. Only six said that TAD rather did not develop their competences, and two said that it did not at all develop their competences. One trainee compared the virtual simulation-based training to be like a real incident. Another commented that, '*Because there are few available practise opportunities, all kinds of command training is very much expected and is highly useful*'. This goes along with IC expectations that have been expressed in the engagement and motivation study (N = 224), which showed that 59% of them would like TAD-style training days once a year, and 24% preferred twice a year. Contradictory to this was the 5% who in the same study expressed their view that this form of training experience is not required.

Earlier, Table 3 in its final two columns provided average figures for IC simulation-based assessment results. We analysed this using a paired T-test to show that IC SA levels average scores that are significantly

different between the first and second time of participating in a TAD. There was no statistically significant difference between the averages for SA levels. On the one hand, it shows that ICs do not get to practice SA enough, and more training opportunities are required in order to improve SA. On the other hand, it shows that the assessment process is carried out consistently by certified assessors, so the results do not differ due to the measurement instrument. In addition, the absence of a significant difference could be positive. It shows that sufficient experience from real life incidents or training are gained, so SA levels have not dropped significantly between assessments.

Due to the fact that TAD is in line with the rescue unit leaders occupational qualification standard, it continually measures the command competences of ICs in the Estonian Rescue Board. Some ICs have left their job after new attestation was implemented, and novices have started to work in their place. TAD allows the service being offered to the public to be screened through a process of monitoring the commanding knowledge and skills of the ICs. Furthermore, from the Estonian Rescue Board perspective, TAD ensures that the occupational qualification command competences of rescue unit leaders are monitored in a systematic way. This allows virtual simulation-based scenario topics and e-learning self-check test questions to be tailored to organisational needs.

5. STUDY LIMITATIONS

The study has several limitations. TAD participants who responded to surveys may have answered as would have been expected or they may have answered with a presumption towards correctness rather than relying on their own feelings. In the survey, to measure trainee reactions, respondents could not provide reasoned argument to support the answers, which could have led to extreme high or low results with no qualitative reasoning behind them. The feedback questionnaire made it possible to comment on the answers being provided. However, only some respondents made use of this opportunity. For this article, the full qualitative analyses behind all of these answers has not been included.

Consideration needs to be taken of the fact that IC answers in the engagement and motivation study did not have the normal level of distribution due to the ceiling effect. It is impossible to distinguish whether a high engagement level and potential well-met psychological needs were the result of there being only a small group of participants, or whether this was due to the efforts of the instructors, or to new methods and tools being used, or due to the assessment at the end of the training session, something that is part of any obligatory work-based attestation.

Another limitation of the study is also the fact that the surveys and assessments were all carried out in the Estonian language. The results are presented in English, and some meanings may be lost in translation. Likewise, in some cases more than two years had passed between taking part in the TAD and filling in the engagement and motivation survey. This may influence answers, as participants had to remember events from a training course from some time previously.

Over 114 ICs in Estonia have twice taken part in TAD, but only those assessment results starting from 2017 have been analysed in the study. This means that the evaluation of TAD participant reactions and learning is not entirely accurate because pilot year assessment results from 2016 were not used. The assessment certificates are always signed by two assessors although, even so, they are filled in using a single EC assessor account. This could lead to a situation in which one assessor has

influenced the scores more than the other assessors. Certain assessor pairs may be able to measure SA levels differently from other pairs of assessors.

CONCLUSIONS AND RECOMMENDATIONS

The research question for the study was how can situational awareness training be provided to ensure different levels of situational awareness as part of dynamic decision-making training using virtual simulations?

In the article, a step-by-step overview was designed and implemented regarding how best TAD can teach about SA levels. We have highlighted the fact that assessor training is key to building engaging virtual simulation-based scenarios and in delivering training that supports all of the psychological basic needs (autonomy, competence, and relatedness). The study proved that TAD is engaging and that it supports trainee psychological needs. XVR OS is used during TAD in a way that means it has allowed ICs to feel engaged and that it supports the learning of SA. Unfortunately, the TAD is not easily scalable, as there are two trainers for each trainee to be able to train and assess SA levels.

Analyses which were based on the Kirkpatrick training programme evaluation model showed that TAD meets Level 1 reactions in a highly positive way. Compared to the motivation and engagement study in clinical settings (Knight, 2016, p. 92) where the clinical engagement mean for students was 5.88 and the SD was at 0.85, TAD showed similar engagement means (M = 5.43 and SD 0.78). We concluded that all three psychological needs (autonomy, competence, and relatedness) are well met during TAD and this serves to support learning in all three SA levels (Kirkpatrick Level 2). From an SA perspective, the Level 3 behaviour and Level 4 results were hard to measure. Other researchers have come to a similar conclusion about simulation-based training (Prohn and Herbig, 2020). Further research is needed in this area. As simulations can be used to measure SA levels (Endsley, 1995a), the EC formal assessment results could be used to evaluate the behavioural changes of participants. As the real-life incident rate is dropping, it is rather difficult to measure IC SA levels during accidents. In future research, which is conducted to discover real-life SA levels, footage could be analysed from the helmet-cams that are worn on IC helmets during incident command situations (Boehm, 2017).

Some trainees found the virtual simulation to be hard to use during TAD. As SA also depends upon the space in which it is taking place (Endsley, 1995a), more research is needed on the area in which virtual simulations are being used to measure different SA levels. Meanwhile, as ICs would expect, more practice opportunities in virtual simulation-based SA training should be provided to them.

Moodle tests are useful when it comes to assessing theoretical knowledge about SA. This is an easily-scalable and standardised way in which to train and to carry out e-assessments (Koneru, 2017). However, it could be argued that computer-based testing is very efficient at supporting trainee psychological needs (Hsu, Wang and Levesque-Bristol, 2019), and how engaging a form of learning this is (Yang, Lavonen, and Niemi, 2018). At this point of the development of Moodle and virtual simulations for SA training and assessment, computers are not able to answer IC questions or dynamically adapt the scenario based on IC decisions. Due to this shortfall, human interaction is still needed in the testing of all SA levels. New training tools will have to be constructed to provide engaged learning in online learning platforms that can take into account trainee cognitive, social, and emotive factors (Wang and Kang, 2006). To extend options and opportunities in terms of online learning, virtual reality technology can be used for multi-disciplinary emergency management training (Prasolova-Forland *et al,* 2017).

Because Moodle self-check tests are an efficient way of testing IC knowledge in regard to SA, new questions should be developed for use in self-check tests. The study showed that even simple feedback from the computer prompts the learner to retake the test. Various e-learning scenarios could improve SA levels 1 and 2, as those average figures were still on the threshold. We suggest that the Moodle platform should be studied in relation to training for command competences that are based on scenarios where the standard operational procedures are applied. With such use, scenarios could be assessed by computer and automatic feedback can be provided for trainees. More research is needed in this area, though, such as how different SA levels may be evaluated via e-learning. When focusing on how assessment results could be used to frame new personal learning-goals and to provide ICs with more options when it comes to reflecting on the e-learning platform before their face-to-face assessment day takes place. One reason for developing e-learning-based training and

the assessment of SA is that it is an easily-scalable way of being able to train ICs in a standardised way.

We concluded that TAD has succeeded in outcome-based, student-centred, virtual simulation and scenario-based training and assessment for all three SA levels. TAD offers a motivating and engaging way in which to train, while the full command competence of ICs can still be challenged. TAD should be continued to assess IC SA levels in virtually-simulated complex incidents. Further research needs to be carried out to be able to find ways in which different SA levels can be taught and assessed in more scalable ways with the aid of virtual simulations.

ACKNOWLEDGEMENTS

We would like to thank the Estonian Rescue Board and EASS for funding IC training in Estonia. We appreciate the vision of Andres Mumma when it came to starting new IC attestation, and would like to thank all of the TAD participants for providing us with context for SA research. We feel we have to praise Andre Tammik for his dedication in TAD implementation and for conducting the engagement and motivation study, as well Kairi Pruul for making sure that the study results were reported at high levels of quality. We struggle to express our profound thankfulness for all of the work of the assessors during TAD, and Katherine Lamb's efforts in training and certifying assessors.

Contacts:

Stella Polikarpus
Estonian Academy of Security Sciences
E-mail: stella.polikarpus@sisekaitse.ee

Tobias Ley
Tallinn University
E-mail: tobias-ley@tlu.ee

Katrin Poom-Valickis
Tallinn University
E-mail: katrinpv@tlu.ee

REFERENCES AND SOURCES

Allas, H. *et al.* (2018) 'Päästemeeskonna juht, tase 5'. Tallinn: Kutsekoda, p. 5. Available at: https://www.kutsekoda.ee/et/kutseregister/kutsestandardid/10684934.

Boehm, M. (2017) "Struck' in the midst of action: incident commanders from Denmark handling everyday emergencies', *International Journal of Emergency Management*, 13(3), p. 272. doi: 10.1504/IJEM.2017.085028.

Chermack, T. J. (2003) 'Mental Models in Decision Making and Implications for Human Resource Development', *Advances in Developing Human Resources*, 5(4), pp. 408–422. doi: 10.1177/1523422303257373.

Cohen-Hatton, S. R., Butler, P. C. and Honey, R. C. (2015) 'An Investigation of Operational Decision Making in Situ: Incident Command in the U.K. Fire and Rescue Service', *Human Factors*, 57(5), pp. 793–804. doi: 10.1177/0018720815578266.

Effective Command (2020) *Effective Command, Effective Command*. Available at: https://www.effectivecommand.org/.

Endsley, M. R. (1995a) 'Measurement of Situation Awareness in Dynamic Systems', *Human Factors: The Journal of the Human Factors and Ergonomics Society*, 37(1), pp. 65–84. doi: 10.1518/001872095779049499.

Endsley, M. R. (1995b) 'Toward a Theory of Situation Awareness in Dynamic Systems', *Human Factors: The Journal of the Human Factors and Ergonomics Society*, 37(1), pp. 32–64. doi: 10.1518/001872095779049543.

Endsley, M. R. (2000) 'Theoretical Underpinnings Of Situation Awareness: A Critical Review', in Endsley, M. R. and Garland, D. J. (eds) *Situation Awareness Analysis and Measurement*. Lawrence Erlbaum Associates Publishers. doi: 10.1002/hfm.1021.

Fire Central Programme Office (2020) *Incident command*. Available at: https://www.ukfrs.com/index.php/guidance/incident-command (Accessed: 12 September 2020).

Girard, C., Ecalle, J. and Magnan, A. (2013) 'Serious games as new educational tools: how effective are they? A meta-analysis of recent studies', *Journal of Computer Assisted Learning*, 29(3), pp. 207–219. doi: 10.1111/j.1365-2729.2012.00489.x.

Groenendaal, J. (2015) *Frontline Command*. The Hague: Eleven International Publishing.

Hariduse Infotehnoloogia SA (2020) *HITSA Moodle*. Available at: https://moodle.hitsa.ee/ (Accessed: 31 May 2020).

Hsu, H.-C. K., Wang, C. V. and Levesque-Bristol, C. (2019) 'Reexamining the impact of self-determination theory on learning outcomes in the online learning environment', *Education and Information Technologies*, 24(3), pp. 2159–2174. doi: 10.1007/s10639-019-09863-w.

Kirkpatrick, D. and Kirkpatrick, J. (2006) *Evaluating Training Programs: The Four Levels*. 3rd edn. San Francisco: Berrell- Koehler Publisher. Available at: https://books.google.ee/books?id=BJ4QCmvP5rcC&lpg=PR9&ots=Mn0_91w_7V&lr&pg=PP1#v=onepage&q&f=false (Accessed: 22 May 2020).

Knight, A. W. (2016) *A self-determination theory-based analysis of the effects of clinical instructor behavior on student clinical engagement, Dissertation/ Thesis*. University of Iowa. Available at: https://ir.uiowa.edu/etd/3123/.

Koneru, I. (2017) 'Exploring moodle functionality for managing Open Distance Learning e-assessments', *Turkish Online Journal of Distance Education*, 18(4), pp. 129–141. doi: 10.17718/tojde.340402.

Kutsekoda (2020) *Kutsestandardid – Kutseregister*. Available at: https://www.kutseregister.ee/et/standardid/standardid_top2/? (Accessed: 29 May 2020).

Lamb, K. et al. (2020) 'Systematic Incident Command training and Organisational Competency', *International Journal of Emergency Services*, in press.

Lamb, K., Boosman, M. and Davies, J. (2015) 'Introspect model: Competency assessment in the virtual world', *ISCRAM 2015 Conference Proceedings - 12th International Conference on Information Systems for Crisis Response and Management*, (August 2005), pp. 235–243. Available at: http://www.scopus.com/inward/record.url?eid=2-s2.0-84947771428&partnerID=tZOtx3y1.

Launder, D. and Perry, C. (2014) 'A study identifying factors influencing decision making in dynamic emergencies like urban fire and rescue settings', *International Journal of Emergency Services*, 3(2), pp. 144–161. doi: 10.1108/IJES-06-2013-0016.

Põder, S.-F., Savimaa, R. and Link, M. (2015) 'A framework for training internal security officers to manage joint response events in a virtual learning environment.', *Proceedings Estonian Academy of Security Sciences: Sustained Security*, pp. 151–180. Available at: https://digiriiul.sisekaitse.ee/bitstream/handle/123456789/131/Proceedings 2015.pdf?sequence=1&isAllowed=y.

Polikarpus, S. (2016) 'Esimese juhtimistasandi teenistujate hindamine ja arendamine', *Täiendõppe õppekava*. Sisekaitseakadeemia, pp. 1–3.

Polikarpus, S. (2017) 'Esimese juhtimistasandi teenistujate kordushindamine', *Täiendõppe õppekava*. Sisekaitseakadeemia, pp. 1–3.

Polikarpus, S., Bøhm, M. and Ley, T. (2019) 'Training Incident Commander's Situational Awareness—A Discussion of How Simulation Software Facilitate Learning', in Väljataga, T. and Laanpere, M. (eds) *Digital Turn in Schools—Research, Policy, Practice*. Singapore: Springer, Singapore, pp. 219–234. doi: 10.1007/978-981-13-7361-9_15.

Prasolova-Forland, E. *et al.* (2017) 'Active learning modules for multi-professional emergency management training in virtual reality', *Proceedings of 2017 IEEE International Conference on Teaching, Assessment and Learning for Engineering, TALE 2017*, 2018–Januar(December), pp. 461–468. doi: 10.1109/TALE.2017.8252380.

Prohn, M. J. and Herbig, B. (2020) 'Evaluating the effects of a simulator-based training on knowledge, attitudes and driving profiles of German ambulance drivers', *Accident Analysis and Prevention*. Elsevier, 138(February), doi: 10.1016/j.aap.2020.105466.

Ryan, R. M. and Deci, E. L. (2000) 'Intrinsic and Extrinsic Motivations: Classic Definitions and New Directions', *Contemporary Educational Psychology*, 25(1), pp. 54–67. doi: 10.1006/ceps.1999.1020.

Ryan, R. M. and Deci, E. L. (2017*) Self-Determination Theory: Basic Psychological Needs in Motivation, Development, and Wellness, The Guilford Press*. Edited by K. W. Brown, D. J. Creswell, and R. M. Ryan. New York.

Smidt, A. *et al.* (2009) 'The Kirkpatrick model: A useful tool for evaluating training outcomes', *Journal of Intellectual and Developmental Disability*, pp. 266–274. doi: 10.1080/13668250903093125.

Tammik, A. (2019) *Õpimotivatsiooni ja kaasahaaratuse tegurite kaardistus päästetöö juhtide arendamisel ja hindamisel*. Sisekaitseakadeemia sisejulgeoleku instituut. Available at: https://digiriiul.sisekaitse.ee/bitstream/handle/123456789/2230/2019_Tammik .pdf?sequence=1&isAllowed=y.

Wang, M. and Kang, M. (2006) 'Cybergogy for engaged learning: A framework for creating learner engagement through information and communication technology', in Hung, D. and Khine, M. S. (eds) *Engaged Learning with Emerging Technologies*, pp. 225–253. doi: 10.1007/1-4020-3669-8_11.

Williams-Bell, F. M. *et al.* (2015) 'Using Serious Games and Virtual Simulation for Training in the Fire Service: A Review', *Fire Technology*, 51(3), pp. 553–584. doi: 10.1007/s10694-014-0398-1.

XVR Simulation (2020) *XVR Virtual Reality training software for safety and security*. Available at: http://www.xvrsim.com/ (Accessed: 29 March 2018).

Yang, D., Lavonen, J. M. and Niemi, H. (2018) 'Online Learning Engagement: Critical Factors and Research Evidence from Literature', *Themes in eLearning*, 11(1), pp. 1–22. Available at: http://files.eric.ed.gov/fulltext/EJ1204753.pdf (Accessed: 26 May 2020).

THE INSTRUMENTALISATION OF THE MASS MEDIA IN RUSSIA'S FOREIGN POLICY: COLD WAR VERSUS CONTEMPORARY STRATEGY

Tomáš Mareš, MA
Charles University in Prague
Institute of International Studies
Faculty of Social Sciences
Department of Russian and Eastern European Studies
Postgraduate Studies

Keywords: Russia, foreign policy, strategy, mass media, psychological warfare, propaganda, soft power, cultural diplomacy, information warfare, weaponized media

INTRODUCTION

The manner in which the Russian Federation (henceforth often referred to here as the 'RF') utilises the power of information in compliance with its foreign policy objectives has become a frequently-discussed issue in the last few years. This debate has been reignited by the significant role that the Russian mass media played throughout the Ukrainian conflict which broke out in 2013 (Badrak and Kozlov, 2016; Carpenter, 2017; Mölder and Sazonov, 2018; Pynnöniemi and Rácz, 2016).[1] Since then, numerous works have emerged which have striven to assess the character of the Russian approach to the instrumentalisation of foreign mass media on the information-psychological level. In the backdrop of this debate, two dissonant strands have formed in this research area. The first group of authors has referred to the current Russian *modus operandi* in this field as a new phenomenon (Giles, 2016b; Rutenberg, 2017; Tolz and Teper, 2018; Bērziņš, 2019). On the other hand, some papers assert the fact that, in recent times, Russia first and foremost has revived old practices that were developed and tested during the Cold War period, thereby neglecting, to some extent, any claims of a new phenomenon (Ajir and Vailliant, 2018; Cull *et al,* 2017; Snegovaya, 2015; Kuzio, 2019). As a result, two more or less conflicting paradigms concerning the nature of the current Russian approach to the instrumentalisation of foreign mass media have been established in the academic discourse. Despite the increased interest in the issue, a study is still missing which would offer a consistent and systematic analysis, and which would strive to contribute to a solution for these contradictions stemming from the associated literature. This encourages further research to be undertaken which may lead to a better conceptual understanding of how the strategy behind the instrumentalisation of foreign mass media on the information-psychological level which was employed by Soviet Russia during the Cold War period differs from the strategic toolset being utilised nowadays by the RF.

In an attempt to address this lacuna, the article uses a diachronic perspective to carry out a variation-finding comparative analysis which will

[1] This paper uses a generally accepted definition of the term 'mass media' to refer to a set of various forms of media-based technology which allows mass communication, or transferring information content to the wider general public.

reveal the essential differences between the Soviet and current Russian strategies behind the instrumentalisation of foreign mass media on the information-psychological level. This perspective enables us to compare the approaches that have evolved over time in terms of Russian strategic thinking and generate a set of differentiating attributes which could determine the character of individual strategic designs. The article sets up four categories that outline the framework for analysis: a) conceptions (creating the rationale for mass media employment); b) mechanisms (techniques of employment within individual conceptions); c) methods of implementation (the application of mechanisms in practice); and d) goals (representing the expected outcomes). These categories are derived from the general definition of 'strategy' that is understood as referring to a plan (involving conception and mechanisms) which delineates the manner (involving methods of implementation) in which one uses their best means (via instruments and/or resources) to achieve the desired end (goals) (Mintzberg *et al,* 2002; Freedman, 2015). This procedure offers a structured examination of the crucial components constituting a strategic design and makes it possible to generate differentiating attributes in regard to the fundamental layers of a strategy formulation. In this manner, the article explains the variation in the characters of those approaches that have been examined against the instrumentalisation of foreign mass media as a direct consequence of a unique configuration in the structure of individual strategic designs. In that respect, the article suggests that different configurations for the crucial layers of a strategy formulation produce varying sets of differentiating attributes that, in turn, provide the strategic designs with specific characteristic features, and yield qualitatively distinctive modalities.

The article is comprised of four chapters matching the categories that have been listed above for analysis, with all of the chapters being structured in the same way. Each chapter begins with a description of the relevant component that forms part of the Soviet strategy in terms of the instrumentalisation of foreign mass media in the appropriate category. The description is used to generate specific differentiating attribute(s) which serve to determine the character of the strategy for the corresponding layer. This step is immediately followed by the same technique that is employed to derive differentiating attribute(s) which serve to determine the character of those strategic modalities that have been utilised by the Russian Federation in recent times at the equivalent level. The

comprehensive sets of differentiating attributes which determine the variation in the characters of individual strategic designs are presented and interpreted in the discussion which concludes this article.

1. CONCEPTIONS

The strategy that involves the instrumentalisation of mass media in foreign policy which was used by Soviet Russia throughout the Cold War era, the rudiments of which were laid down in the late 1940s, was based on the concept of psychological warfare (Nietzel, 2016). From a holistic perspective, psychological warfare includes political, diplomatic, economic, and military actions, along with mass media information streaming in the enterprise to enforce one's will over that of the opponent, embracing the resultant power relations in the form of domination (Smith, 1953). In reference to psychological warfare, mass media is only one of a variety of tools that can produce an influence on the thoughts and actions of the target audience, whether they are meant to be political leadership members, specific segments within a population, or the general masses (Finch, 2000). Psychological warfare which has been conducted through mass media incorporates techniques to influence the belief system of the target foreign audience, along with its emotions, motivations, or reasoning, to induce confessions, reinforce attitudes, and provoke shifts in human behaviour that may be favourable to the state entity that employs this technique. Through this means, psychological warfare is meant to interfere with mental perception by intervening in the cognitive processes of the target audience (Doob, 1949). The key to understanding the Soviet strategy of the instrumentalisation of foreign mass media is embedded in Marxist-Leninist ideology which grew for decades, inseparable from the concept of psychological warfare (Thompson, 1989; Pechatnov, 2001). For this reason, in the Cold War period, psychological warfare was understood as a means of non-military confrontation which had a substantially limited but still offensive nature. The offensiveness was not imminent; instead, it was hidden deep in the very essence of Marxism-Leninism, and it consisted of the effort to little-by-little strike at public discourse in the target countries and preponderate political support on the side of Soviet Russia or its sympathising groups (CIA – Office of Soviet Analysis, 1955). Mass media became an instrument that could be used to enforce an ideological struggle by encouraging dichotomised reality that portrayed a world which had been divided into two camps: the Soviet camp of social-economic equality, democracy, and peace against the Western world of the bourgeoisie, with its autocracy, conflicts for resources, and

war. Russian media promoted the vision of socio-economic order that was provided by Marxism-Leninism and defamed any other competing alternative (Bessonova, 2010). In short, the Soviet strategy, which was based on the concept of psychological warfare, was characterised by two mutually related differentiating attributes: an overarching ideology with a limited (but still) offensive character.

After the end of the Cold War, and with the dissolution of the Soviet Union and the rejection of Marxism-Leninism as a dominant theory which could shape the Russian worldview, the expert community in the newly-established multi-ethnic and multicultural Russian Federation formed an innovative perspective on Russian identity and its role in the changing international environment, which was termed the Russian World (Suslov, 2017).[2] Against this background, Russia started a process of forging a national identity by (re)constructing the discursive boundaries of nationhood. It did so by invoking a particular vision of what constitutes a new imagined nationalised political community and by promoting this amongst the population through speeches, interviews, various state agencies, and within the wider media landscape (Bolin, Jordan, and Ståhlberg, 2016). The foreign policy conception that was based on the Russian World construct, which has been saturated by neoconservative values with nationalistic overtones, has constituted a new ideational framework and has become the cornerstone of Russian soft power (Laruelle, 2015a; Suslov, 2017; Tiido, 2015). However, Russian political leaders have primarily interpreted soft power in a very instrumental manner (Laruelle, 2015a; Sergunin and Karabeshkin, 2015). As is maintained by the broader definition that distinguishes between the state-led category and the civil-society-led category, soft power can intentionally be employed by state institutions in compliance with foreign policy goals. Therefore, a country may achieve the outcomes it wants not solely because others admire its values, but also by deliberately setting an agenda (Burlinova 2015; Watson 2012). In the realm of international politics, the soft power, which combines the Russian World and neoconservative values, has retaken the role of an overarching ideology. This ideology has enabled an increase of

[2] The Russian World incorporates the following population segments: a) ethnic Russians who are living within the borders of the RF; b) residents of the RF who are not ethnic Russians; c) ethnic Russians who are living outside the RF's territorial borders; and d) non-Russians who are living outside the RF but who associate themselves with its cultural-historical heritage (Zevelev, 2001; Tiido, 2015).

Russia's foreign policy influence by employing enough vague and alluring combinations of cultural and value-based agendas with the potential to address sympathising groups among foreign populations no matter in which part of the world they live (Suslov, 2017; Wilson, 2015). Russia resorts to this ideological framework to bring together the interests of various ideationally associated groups, to encourage new or closer cooperation with other states or sub-state political entities, and to enhance support or legitimacy for particular actions (Lenczowski, 2009). With respect to mass media streaming, Russia interconnects the cultural value-based agendas with the effects of the expansion of large media corporations into foreign media markets (Laruelle, 2015a; Dimitrova *et al,* 2017). Thanks to this, soft power which can be channelled through mass media assets is treated rather as a source of international connections that help to facilitate an association with Russian interpretations of reality in the most prone segments within the target foreign audience (Zeleneva and Ageeva, 2017). In contrast to the role of Marxism-Leninism in the Cold War era, this conception is not engaged simply to combat hostile regimes, but to build transnational communities that are related to the RF by means of shared values, culture, and traditions (Keating and Kaczmarska, 2019). In this regard, the function of the current ideological framework, which is based on an amalgam of the Russian World and neoconservative values, fundamentally differs from the role of Marxism-Leninism in Cold War-era psychological warfare. As a result, the current Russian strategy, which is based on the concept of soft power, has been characterised by the following differentiating attributes: as an overarching ideology with a non-aggressive unifying nature.

Following the war in Georgia in 2008, experts in Russian military circles fully entered the debate. Russia has developed a renewed and progressive approach that should help it to win contemporary interstate conflicts, those in which a military confrontation has been marginalised to minimum rates, and non-military means have become the primary instruments of attacking the enemy to tamp down its ability to resist: new-generation warfare in its essence (Ermus and Salum, 2016; Rotărescu, 2015). As a consequence, Russia integrated information measures into the essential components of its contemporary warfare alongside military force, special forces missions, or economic measures (Hellman and Wagnsson, 2017; Pynnöniemi, 2018). This gives Russia an offensive capacity in times in which the public tolerance of military intervention

has rapidly decreased (Franke, 2015; Fedyk, 2017). In this context, the conception of information warfare provides a framework which can serve to drive the instrumentalisation of foreign mass media that fits with the changing Russian attitude to international conflict resolution which is provided by this sort of militaristic reasoning (Cockrell, 2017). The concept of information warfare is now understood in a purely offensive and utilitarian manner. This approach is deprived of any ideological obligations, as it is driven strictly by the principle of effectiveness (Thomas, 2016). Mass media assets are activated *ad hoc*, and with varying levels of intensity they are used to disseminate customised narratives that suit the desired intentions which themselves can differ significantly in individual media markets (Braghiroli and Makarychev, 2017; Ellehuus, 2020; Mankoff, 2020). The aim is not to provide a sole, unified narrative structure as given by Marxism-Leninism or the Russian World construct, but rather to create several customised narratives in order to give rise to the clashing preferences of different segments within a population in target states. Different audiences are targeted with different messages, as different societies can be fragmented by different issues (Fedchenko, 2016). Therefore, the contemporary strategic design of the instrumentalisation of foreign mass media that has been built up in the concept of information warfare that is rooted in the militaristic thinking that has been detailed above makes it possible for Russia to carry out information-based assaults that serve to exploit a full scale of locally unique social, cultural, economic, or political community problems (Lucas and Pomerantsev, 2016). This approach is in sharp contrast with the Cold War conception of psychological warfare, which strived gradually to erode political regimes by employing generalised ideological content given by Marxism-Leninism in a long-lasting systemic rivalry (Bolsover, 1948; Barghoorn, 1964). Taking all this into account, the current Russian strategy, which is based on the concept of information warfare, has been characterised by the following differentiating attributes: theatre-based opportunism (deprived of any ideological doctrines) in combination with a purely offensive nature.

2. MECHANISMS

The pivotal mechanism in the field of the instrumentalisation of foreign mass media within the framework of the concept of psychological warfare adopted and refined by Soviet Russia was propaganda (Nietzel, 2016). Propaganda is a process which serves to exploit the psychological effects of information dispersion that could concisely be defined as a set of systematic, deliberate communications practices that attempt to shape perceptions, and manipulate cognitions and direct behaviour to achieve a response that furthers the desired intent (Jowett and O'Donnell, 2012). Most of the propaganda definitions are rooted in three fundamental features: direct social control; a narrowing of decision-making options; and explicit appeal to enforce change (Carey, 1996; Merrill and Lowenstein, 1971; Qualter, 1962). This requires the information message to be framed to significantly limit the space for opinion-making and channel the content in a considerably constrained manner which serves to close minds, does not allow questions, and leaves no alternative to choose from other than the one demanded by the propagandist (Black, 2001). In that respect, propaganda is unanimously defined as a deliberate attempt to form, control, and alter the attitudes of the target audience in such a manner that, in any given situation, the reaction of those so influenced will resemble the one desired by the propagandist (Carey, 1996). Soviet foreign propaganda was used as a mechanism of enforcement, as it deliberately strived to manoeuvre the target audience to accept the Marxist-Leninist worldview. Therefore, propaganda turned out to be a mechanism that was designed to lead the non-military confrontation in the geopolitical conditions of the Cold War (CIA - Office of Soviet Analysis, 1955). Information-psychological operations within the propaganda framework were designed to achieve as much direct social control over the target foreign audience as was possible to produce maximum social manoeuvring that could be carried out through the dispersal of information content and to directly guide the change in public discourse regarding a bipolar ideological confrontation that favoured the Soviet perspective (CIA - Office of Soviet Analysis, 1955; Darczewska, 2014). With this in mind, we can claim that the logic behind social control which enables direct public management became the critical differentiating attribute that served to characterise propaganda as

a mechanism of the instrumentalisation of foreign mass media within the framework of the Soviet-style concept of psychological warfare used in the Cold War period.

If we switch our attention to the current Russian strategy, cultural diplomacy functions as a mechanism which provides a meaningful framework for mass media instrumentalisation in terms of the concept of state-led soft power (Simons, 2013). Russian mass media came to be understood as a bearer of a message that contained a culturally-tainted and value-based ideology which served to reinforce the country's political agenda; it has become a source of gravitation in terms of building links to its foreign audience (Rotaru, 2017). In that context, Russian cultural diplomacy simply employs different forms of manipulation by using mass media content to address communities at both civic and state levels in an effort to bind them with its cultural/value model and engage them in its foreign politics. This is why some authors classify such a practice as cultural propaganda or neo-propaganda (Jang, 2019; Zamorano, 2016; Zeleneva and Ageeva, 2017). The neo-propagandist approach suggests the intention to win over the public in terms of particular interests through a massive orchestration of seductive conclusions that are packaged to conceal their persuasive purpose (Sproule and Lewis, 1994). However, Russian cultural diplomacy differs from the Soviet-style propaganda in at least two important aspects: a) it is not a mechanism of enforcement; and b) it does not strive to maximise social control through managing public discourse by extensively narrowing the public space for decision-making (Melissen, 2005; Lenczowski, 2009). While Cold War propaganda directly enforced the target audience to embrace the one and only possibility of change that was being predefined by the information content, the current form of Russian cultural diplomacy is less insistent, looser, and more vague. It is much more dependent upon self-identification (Laruelle, 2015b). Russian cultural diplomacy, which is channelled through mass media, calls for support or active participation in a multi-national, inter-religious, Russia-centric civilisation-strengthening collective identity that is based on ideals of human rights, faith, spirituality, kindness, conservative ethics and/or morality, conscience, and a traditional attitude to sexuality in association with family life (Feklyunina, 2016). Cultural diplomacy in the form that is currently being employed by Russia rather tries to arouse sympathies for the proposed values and/or cultural framework that is embodied in the

Russian World construct, and which provides the target audience with the chance of becoming part of it (Laruelle, 2015a). It sounds more like an offer or an invitation. Cultural diplomacy relies on indirect influence; hence, it can provide much less straightforward control over decision-making in the ranks of the target audience when compared to Cold War propaganda driven by Marxism-Leninism (Klyueva and Mikhaylova, 2017). With that being said, the logic of social convergence that leads to the establishment of transnational communities has become the central differentiating attribute that characterises cultural diplomacy as a mechanism of the instrumentalisation of foreign mass media within the framework of the soft power concept that is being utilised by the RF.

The mechanism behind the Russian concept of information warfare is weaponised media, which incorporates the entire scale of mass media technologies ranging from traditional newspapers and all types of broadcasting media, up to the new forms of social media (operating on internet platforms) which play a substantial role as multipliers of the impact of information streaming (Nissen, 2015; Partanen-Dufour, 2016). In this vein, mass media sources are considered to be an essential weapon through which a decisive offence that can capitalise on the information-psychological effects of massively dispersed information narratives can be launched in peaceful conditions as well as during wartime (Flemming, 2017). The core message of this changing strategic reasoning is the following: while traditional combat remains a possibility, it will no longer be the primary means of victory on the battlefields of the twenty-first century. In contemporary Russian strategic thinking, information warfare with a substantial position in mass media has taken over the reins (Bērziņš, 2019). The idea of a weaponised media goes beyond the propaganda framework. This is not about the propagation of any specific worldview, but more about the opportunistic utilisation of information to be able to strike the weakest or most sensitive points within the structure of the populations of the target states (Giles, 2016a; Pomerantsev and Weiss, 2014). Instead of gaining social control, weaponised media sources use information to carry out precisely aimed assaults which can seriously harm the target states by disrupting popular discourse, causing public disarray, and decreasing the ability of the affected population to assess the real state of affairs (Lucas and Nimmo, 2015). Therefore, mass media sources are employed to cause as many destructive, damaging, or detrimental effects as possible by

breaking consonance in the ranks of the target society across a variety of issues that are at hand (Doroszczyk, 2018; Szostek, 2017). From this perspective, the logic behind social fragmentation, which is motivated by a desire to cripple the social integrity of target states, is the primary differentiating attribute that serves to characterise a weaponised media as a mechanism of the instrumentalisation of foreign mass media within the framework of the concept of information warfare.

3. MEANS OF IMPLEMENTATION

At the level of practical implementation, Soviet foreign propaganda utilised the principle of ideological indoctrination. According to the common definition, the purpose of ideological indoctrination is to imbue the target audience with theories, doctrines, and beliefs that are provided by specific thinking in a dogmatic, unquestionable manner (Lammi, 1997). In the Soviet reality, ideological indoctrination worked on persuasion, as it strived to force the target audience to adopt the picture being presented to it in a way that was consistent with the underlining thoughts that were epitomised in Marxism-Leninism whilst at the same time constructing an image that portrayed a new state-social configuration and blackened competing alternatives (with capitalism/imperialism in the first place) (Cassinelli, 1960; Brandenberger, 2011). Although Soviet persuasion also used a positive form of motivation (an image that provided more than simply social order) within the framework of competing paradigms, and therefore, it encouraged self-identification to some extent, the practice of indoctrination did not leave any space for free independent decision-making. The target audience was not expected to question or critically examine the doctrine they had learned, but were supposed to accept it as an objectively-given reality. Soviet propaganda, which was based on persuasion through ideological indoctrination, demanded full-scale commitment; it appealed either for the recipient to be a follower, or to become a foe who must be defeated (Barghoorn, 1964; Brandenberger, 2011). This technique was designed to instil intentionally biased ideas into human minds to force people to behave according to the will of the propagandist while refusing any independent choice or doubt (Schweitzer, 1962). Therefore, persuasion here is perceived as a process through which one state imposes its beliefs on another by manipulating the target state's population through the means of deliberately created and ideologically-tainted information campaigns (Jowett and O'Donnell, 2012). Moreover, Soviet propaganda, which was based on persuasion through ideological indoctrination, portrayed international relations in a polarised perspective which invoked a vision of a world that was divided by pervasive and non-avoidable conflict embodied in the struggle between Marxism-Leninism and any other competing socio-economic or political theory (Brzezinski, 1960; Papp, 1979). The practice of indoctrination mixed with the polarised

worldview forced the target audience to think of international relations as a zero-sum game by drawing a world in which cooperation amongst states with differing ideological affiliations was not an acceptable possibility. As a consequence, Soviet foreign propaganda produced an image that showed social relations as a constant struggle for power domination and urged people to fight for the sake of Marxism-Leninism (Zimmerman, 1969; Buecker, 2003). Against this background, differentiating attributes which determined the specific character of Soviet Cold War propaganda have emerged at the level of practical implementation: dogmatism which encouraged an antagonistic polarisation both at the intrastate and the international level.

At this point, we should also turn our attention to the special information operations used in the Cold War era. Derived directly as a specific branch of propaganda, the special information operations in Soviet Russia were labelled 'спецпропаганда' ('special propaganda') (Darczewska, 2014). Special propaganda was employed in the form of: a) active measures, which were usually taken in the form of calculated information leaks that were published with no obvious relation to Soviet Russia or its allied organisations; or b) reflexive control, which intentionally conveyed to an opposing side certain aggregate information which would cause it to make a decision appropriate to the information it had received (Ajir and Vailliant, 2018; Giles, Sherr, and Seaboyer, 2018). Special propaganda refers to the clandestine methods used in enforcing Soviet authority abroad: efforts to control media in foreign countries; written or spoken disinformation which is retranslated by media assets that have been retaken by Soviet proxies in foreign countries; the use of communist parties and front organisations to disseminate information that favours Soviet interests on the ground; illegal transborder radio broadcasting; or information operations that serve to build up pressure on the political leadership (Fedchenko, 2016). As such, special information operations were employed when Soviet Russia attempted to increase the effects of persuasion through ideological indoctrination, especially by concealing links to the Soviet political regime for any disseminated information (Active Measures Working Group, 1987). Former Czechoslovak intelligence officer, Ladislav Bitman, who defected to the west in 1968, describes Soviet-era special information operations as manufacturing forgeries: 'Forgeries […] are classified into two major categories. The first category includes misleading information (disinformation) that contributes to

poor policy decisions among government leaders. This type of fakery usually does not require or receive widespread attention from the media. The second type, propagandistic forgery, seeks to mould public opinion in a target country.' (Bittman 1985, p 96). However, special information operations went only slightly beyond the generalised ideological doctrines and used several basic forms of narrative in many variations, repeating them over and over: a) portraying internal or regional interstate conflicts as a direct outcome of the imperialistic policies of the USA or other western (European) countries within the framework of colonialism, cultural oppression, or economic plundering; b) accusing the USA (or other countries that were labelled as being capitalist or imperialist) of arms proliferation, war-mongering, or supporting alleged terrorist groups; c) displaying the success of social revolutions (such as those taking place in Latin American states) in an effort to support the resolve of people to join the 'nation liberation' that was being led by Soviet sympathisers; or d) defaming figures and organisations that were held in high esteem within society where they opposed ideas that were being put forward by Soviet ideological propaganda (Barghoorn, 1964; Active Measures Working Group, 1987; Staar, 1991). For these reasons, the article understands special information operations as being an integral part of propaganda (as described above), the primary purpose of which was to multiply the effects of dogmatised ideological persuasion.

The form of cultural diplomacy which Russia utilises today is rooted in soft power. It employs persuasion through attraction, inducement, and co-option to shape peoples' actions and motivate them to support Russian policies (Lord, 2009). In contrast to the Cold War era, current forms of Russian persuasion through attraction allow different levels of self-identification. In essence, it does not force people to choose the only 'good' that is predetermined by the media content as did Cold War propaganda. It means that people can fall in with it only partially, to coincide with a limited volume of precisely-chosen pieces of a presented agenda (Rutland and Kazantsev, 2016). It must be mentioned here that Russian persuasion through attraction which employs the previously-defined ideological framework of soft power, which is based on neo-conservatism with nationalistic connotations and which is sometimes labelled as nationalistic neo-conservatism, has often been formulated in opposition to western globalist liberalism (Lukin, 2014; Shcherbak, 2019). Therefore, some arguments suggest that the relationship between

the current Russian nationalist neo-conservatism and western globalist liberalism resembles the geo-ideological polarisation of the Cold War era (Diesen, 2019; Karaganov, 2018), However, despite the nationalist neo-conservatism being promoted by Russia as being set out as an alternative to western globalist liberalism and often criticising liberal values, it lacks the antagonistic tendencies that were embedded in Cold War ideology. Current forms of Russian-led persuasion fall short of a direct appeal to carry out significant changes in the structure of other (competing) political regimes (Keating and Kaczmarska, 2019; Kortunov, 2019). On the contrary, Russian soft power media messaging portrays the Russian World and the value framework it embodies as a unique transnational civilisation that is increasingly endangered by globalisation that is spreading the westernised model of cultural liberalism (Meister, 2016). This is because Russia's soft power is not designed to seek out strategic superiority (Klyueva and Mikhaylova, 2017). In comparison, Russian messaging heavily advocates multipolarity, which can be comprehended as the central feature of any stable world order (Laruelle, 2015b). This vision rejects one or more dominant states when it comes to being able to impose rules on the rest of the world and prefers geopolitical, geostrategic, and geo-economic pluralism (Hinck, Kluver, and Cooley, 2018). Russian narratives are based on the premise that all participants in international relations should respect each other's interests (Stronski and Sokolsky, 2020). Current Russian soft power reasoning upholds the idea of multiplicity and plurality in terms of world cultures, and argues that idiosyncratic cultural qualities must underpin all political systems and structures (Chebankova, 2015). Russian media messaging claims that countries with different socio-economic and political systems can interact peacefully and should play by existing rules. Still, it simultaneously justifies efforts to make international norms more appropriate to national interests. In the end, instead of the Cold War appeal to revolution, Russia's narratives stand for its cultural/value model, claiming the right to preserve equality among countries, and stipulating respect for its state and/or national concerns (Sergunin and Karabeshkin, 2015; Miskimmon and O'Loughlin, 2017). Therefore, Russia does not necessarily see other players as its adversaries, but rather as competitors. This logic portrays international relations as a non-zero-sum game, where multipolarity, peaceful coexistence, and cooperation (especially when taking into account economic affairs) are possible or even desirable options (Sergunin and Karabeshkin, 2015). In contrast to Cold War propaganda, the differentiating attributes determining the

specific character of Russian cultural diplomacy at the level of practical implementation are: self-identification, which allows cultural and political multipolarity both at the intrastate and the international levels.

Weaponised media sources employ traditional methods that were evolved and perfected in the Cold War era (Cimbala, 2014; Snegovaya, 2015; Abrams, 2016). Russia, in this regard, heavily relies on massive volumes of disinformation dispersed in systematic campaigns. It also employs reviewed, rebuilt, and transformed special information operations (Snegovaya, 2015; Lucas and Pomerantsev, 2016). Contemporary special information operations still utilise public figures of the state as primary targets. To undermine the prestige of target state authorities and tamp down their legitimacy, Russia carries out attempts to defame political leaders or reduce belief in their levels of honesty and reliability, or to discredit policies that are incompatible with Russian interests (Doroszczyk, 2018). Besides that, Russia still utilises forgeries and engages proxies that are situated in the target states as influencers to conceal the origin of specific information or disinformation to augment its impact on the affected audience (Ajir and Vailliant, 2018). In this aspect, weaponised media resembles Cold War propaganda. Notwithstanding, Russian media assets use these methods in a considerably distinctive *modus operandi*. Instead of indoctrinating the target audience with ideology or simply misleading it with disinformation, weaponised media sources are designed to attack the enemy directly and to harm the complex intrastate decision-making process in a bottom-up direction by pushing already-existing social grievances, stereotypes, and vulnerabilities (Meister *et al,* 2018). Russian information streaming utilises the full spectrum of available social discrepancies to arouse internal turmoil amongst religiously, culturally, nationally, value-based, or politically diverse segments that exist within the populations of the target states (Fedchenko, 2016). In that regard, the RF proactively utilises information content to spread hate speech, to destroy trust, sap morale, degrade the information space, erode public discourse, increase partisanship, or incite violence (Lanoszka, 2016; Lucas and Pomerantsev, 2016). Such forms of implementation demand extremely focused information narratives with a strong potential to encourage internal disputes between different segments within a target society, while also undermining trust in and the devotion of inhabitants to the central government authority, precipitating upheavals or even armed insurgencies, and 'decomposing' the social-political order from below

(Bruusgaard, 2014). This approach does not strive to persuade the target audience about a specific set of beliefs to generate control over them, but to exploit existing opinion and/or social incongruity to fuel an escalation of internal conflict. This form of implementation is not about achieving direct domination, but is about igniting strong enough division to reverse unfavourable tendencies in the political development of target states. In this sense, weaponised media sources are used to stop political processes that have a potentially negative impact on Russian foreign policy interests, no matter whether they are economic, cultural, or security processes (Bugajski, 2020). For these reasons, the characteristic features determining weaponised media sources in terms of practical implementation are: resentment stimulation producing socio-political disintegration both at the intrastate and international levels (such as narratives that are disseminated by Russian media outlets which target conflicting interests amongst EU or NATO member countries) (Hofmeisterová *et al,* 2018; Ellehuus, 2020; Mankoff, 2020).

4. GOALS

Soviet foreign propaganda was, first and foremost, devoted to a political-ideological mission: overthrowing capitalism, establishing socialism, and building up communism around the world (Bessonova, 2010). Therefore, the ultimate goal of the Soviet strategy was to support the territorial expansionism of the Marxist-Leninist ideology and thereby increase the foreign influence of Soviet Russia around the world to the detriment of its primary foe, the alliance of western states, which labelled as capitalist or imperialist (Marxism-Leninism defines imperialism as the last stage of capitalism) (Kuusinen *et al,* 1963). In Soviet strategic culture, psychological warfare did not solely target the enemy that was embodied in western capitalistic states but also neutral countries that stood in the middle without so far having aligned with either side of the bipolar confrontation (Triska, 1958; Light, 1991). The ultimate goal can be divided into several sub-categories: a) indoctrinate foreign audiences with the Marxist-Leninist ideology (implant sympathies that lead to the formation of groups of supporters who adopt Soviet ideology and persuade a foreign public to believe in systemic flaws within the western capitalistic and/or imperialistic states, such as moral depravation, socio-economic defectiveness, or aggressive expansionism); b) enforce the supporting groups so that they can undermine the political system in their countries and potentially spark off ideologically-motivated (socialist) revolutions; and c) support the process of building socialism in countries in which sympathising groups have retaken political power (Bolsover, 1948; CIA – Office of Soviet Analysis, 1955). In short, this is a revisionistic and non-systemic approach that seeks to change ideologically incompatible regimes and challenges the existing international order in the contest for ultimate victory which will grant the winner hegemonic dominance.

The ultimate goal of the current Russian soft power strategy is to enhance political influence in an environment of peaceful coexistence and to mitigate the negative effects of certain policies in regard to international reputation (Yablokov, 2015). This ultimate goal can be divided into three larger sub-categories: a) positive-image-making; b) legitimacy enhancement; and c) support-searching (Simons, 2014). This specific set of goals is designed to help Russia spread its influence abroad and allows it to

keep up in the geopolitical competition with other great powers like the USA, China, and India, when it comes to diffusing the world with their own socio-cultural paradigms (Isar, 2017; Krenn, 2017; Liu, 2019). In doing so, Russia strives to: a) attract foreign audiences to its socio-cultural value-based agendas; b) excite feelings of self-identification with this ideologised framework; c) encourage the target audience to engage in promoting and preserving this common legacy; and d) co-opt foreign audiences into cultural/political programmes that are organised abroad by Russian institutions (Hudson, 2013). Compared to the Cold War strategy, these goals are soft in nature, as they are short of revisionistic ambitions as well as any appeal for aggression or subversion. Instead, they try to profile the position of the Russian Federation within the boundaries of the existing system. Rather than seeking change or denigrating an enemy, current soft power goals are formulated in mild, unifying, or even appeasing overtones. They support legitimacy enhancement by promoting: a) multilateralism and cooperation; b) culture and values; c) human rights; and d) the historical importance of Russia (Klyueva, 2017). In relation to strategic goals, the current soft power approach tends to be a more-or-less cooperative strategy that seeks to increase Russian influence abroad, while not radically challenging the existing setting in the structure of the international system.

With regard to the concept of information warfare, contemporary Russian strategy derives much more tangible goals than simple regime overthrow. Information campaigns are now targeted at a particular audience in a considerably narrower way and with unprecedented precision, which allows certain levels of flexibility in stating the objectives. Although the current strategy is closely related to the 4D[3] approach, Russia does not strive simply to distort reality or distract attention (these two elements exemplify the primary fields for mass media instrumentalisation in the 4D design), either of the wider public or the political leadership in the target states (Snegovaya, 2015; White, 2016). The goals that are attached to current foreign Russian mass media offensive campaigns are tailor-made to specific conflict situations and to different geopolitical arenas, thereby representing distinctive operational environments (Perry, 2015). This means that the essential purpose of contemporary information campaigns is to paralyse the affected state's capability to

[3] Dismiss-Distort-Distract-Dismay.

mobilise the power that is necessary to counter Russian interests as much as possible in specific operational conditions (Fedchenko, 2016). This is achieved by limiting sources of internal sovereignty, and the extent of any limitation can significantly vary in accordance with specific needs and intentions in individual geopolitical theatres in the following forms: a) inflicting confusion to mitigate public reaction in terms of specific Russian policies; b) arousing the fragmentation of opinion and thereby limiting the space for manoeuvre for the target country when it comes to introducing counter-measures; c) disintegrating the target audience in an effort to paralyse the state's ability to raise internal support; and e) perhaps even initiating turmoil or motivating subversion (Meister, 2016; Pasitselska, 2017). The aim is to unfold the internal instabilities that may exist within individual target states and incite fragmentation processes within the ranks of the target society at the desired level of intensity (Bugajski, 2020). To give an example, this dynamic is particularly evident in the western Balkan states where Russian media exploits issues of frozen conflicts in the region, while also fostering nationalistic sentiment, and reviving inter-ethnic rivalry to thwart the ambitions of local governments to be able to associate themselves with Nato or EU institutions (Stefanov and Vladimirov, 2018). This strategic modality is designed to stop or change political development that is unfavourable to Russia, and thereby to revise the foreign policy course that has been fostered by particular states. Instead of exhibiting ambitions to change the existing structure of the international system, this approach strives to make the international environment more Russia-friendly by suffocating political developments at a national level where such developments have the potential to harm Russia's foreign policy interests. Therefore, we can claim that this strategy is partially revisionistic at the state level, but systemic at the international level.

DISCUSSION

In the Cold War period, solid foundations were set out. These served to drive the systematic utilisation of mass media power in compliance with foreign policy goals. In that regard, the current Russian strategic toolset reinvigorates the Cold War roots, as it strives to employ mass media sources to manipulate the thinking and doing of the target foreign audience through the means of socio-psychological manipulation. In this manner, contemporary Russian strategic modalities utilise information content, which has been massively dispersed into foreign media markets to influence the human perception of reality and to produce changes in behaviour in the ranks of the target audience abroad that is in favour of Russian interests. This article shows that at least two modalities have consequently developed in Russian strategic thinking: soft power and information warfare. It is apparent that the current developmental trends have reflected on some of the key characteristics that determined the nature of Soviet Cold War strategy. While the design of soft power revives the use of ideological content, information warfare restores the offensive reasoning through the means of additional disinformation campaigns and special information operations.

Despite this basic affinity, the diachronic perspective indicates that the Russian strategic toolset in the field of the instrumentalisation of foreign mass media has been progressively adapting to the development of geopolitical conditions. It has responded to the changing position of Russia in the international system, and has directly addressed evolving foreign-policy ambitions. Within this context, the evidence shows that the Russian strategic toolset when it comes to the instrumentalisation of foreign mass media has undergone significant changes following the dissolution of the Soviet Union. The article revealed fundamental differences that stemmed from varying configurations in the crucial layers of strategy formulation. Each of the examined modalities that has developed in Russian strategic thinking over time has been built upon different conceptions that function through distinctive mechanisms that in turn use idiosyncratic means of practical implementation that are tailor-made for achieving a precisely formulated sets of goals. These dissimilarities provided the individual strategic designs with unparalleled

sets of differentiating attributes according to which we can unambiguously distinguish between them. The aggregated sets of differentiating attributes that are generated for the given layers of a strategy formulation, and which serve to explain the variations in the character of individual strategic designs, are summarised in Figure 1.

FIGURE 1.

	cold war strategy	present strategic toolset	
strategic modalities	• psychological warfare based on marxism-leninism	• soft power based on russian world	• information warfare based on militaristic reasoning
conception	• overarching ideology • limited offensive	• overarching ideology • non-aggressive	• opportunistic • purely offensive
mechanism	• social control	• social convergence	• social fragmentation
implementation	• dogmatism • antagonistic polarization	• self-identification • multipolarity	• resentment stimulation • disintegration
goals	• revisionistic (state level) • non-systemic (international level)	• non-revisionistic (state level) • systemic (international level)	• partially revisionistic (state level) • systemic (international level)

These sets of differentiating attributes can be summarised into coherent characteristics that define the examined strategic approaches which have developed over time in Russian strategic thinking.

1. The Soviet Cold War approach to the instrumentalisation of foreign mass media at an information-psychological level, which was constructed on the basis of the concept of psychological warfare, is

characterised as: an ideologically-based offensive strategy that functions on the principle of social control, which is achieved through dogmatic content messaging that promotes antagonistic polarisation. This is a revisionistic, non-systemic strategy that is designed to initiate the overthrowing of incompatible regimes in an effort to gain systemic dominance.

2. The first approach in terms of the instrumentalisation of foreign mass media sources at an information-psychological level, which has been utilised by the RF in recent times and has been built on the concept of soft power, is characterised as: an ideologically-based non-aggressive strategy that functions on the principle of social convergence, which is achieved through self-identification, opening the way for cultural and political multipolarity. This is a non-revisionistic, systemic strategy that is designed to maximise power within a system of peaceful coexistence.

3. The second approach to the instrumentalisation of foreign mass media at an information-psychological level as has been utilised by the RF in recent times and which has been based on the concept of information warfare, is characterised as: an opportunistic, purely offensive strategy that is based on a militaristic rationale which functions on the principle of social fragmentation achieved through the stimulation of resentment to stir up socio-political disintegration. This is a partially revisionistic strategy that is designed to reverse unfavourable policies by particular players whilst not disturbing the existing structure of the international system.

Contacts:

Tomáš Mareš
Charles University in Prague,
Institute of International Studies,
Faculty of Social Sciences,
Department of Russian and
Eastern European Studies
E-mail: tomas.mares@fsv.cuni.cz

REFERENCES AND SOURCES

Abrams, S., 2016. Beyond Propaganda: Soviet Active Measures in Putin's Russia. *Connections*, 15(1), pp. 5–31.

Active Measures Working Group, 1987. *Soviet Influence Activities: A Report on Active Measures and Propaganda.* United States Department of State. pp. 1–87. [Online source] Available from: www.globalsecurity.org/intell/library/reports/1987/soviet-influence-activities-1987.pdf [Accessed 26.01.2020].

Ajir, M., Vailliant, B., 2018. Russian Information Warfare: Implications for Deterrence Theory. *Strategic Studies Quarterly*, 12(3), pp. 70–89.

Badrak, V., Kozlov, D., 2016. *The Kremlin's Information Front*. Center for Army, Conversation and Disarmament Studies.

Barghoorn, F., 1964. *Soviet Foreign Propaganda*. Princeton University Press.

Bērziņš, J., 2019. Not "Hybrid" but New Generation Warfare. In *Russia's Military Strategy And Doctrine* (Howard, G., Cyekaj, M., ed.), pp. 168-172. The Jamestown Foundation.

Bessonova, M., 2010. Soviet Perspective on the Cold War and American Foreign Policy. In *Comparative Perspectives on the Cold War: National and Sub-National Approaches* (Trepanier, L., Domaradyki, S., Stanke, J., ed.), pp. 41-58. Krakow Society for Education: AFM Publishing House.

Bittman, L., 1985. *The KGB And Soviet Disinformation: An Insider's View.* Pergamon Press.

Black, J., 2001. Semantics and Ethics of Propaganda. *Journal of Mass Media Ethics - Exploring Questions of Media Morality*, 16(2–3), pp. 121–137.

Bolin, G., Jordan, P., Ståhlberg, P., 2016. From Nation Branding to Information Warfare: Management of Information in the Ukraine-Russia Conflict. In *Media and the Ukraine Crisis: Hybrid Media Practices and Narratives of Conflict* (Pantti, M., ed.), pp. 3-38. Peter Lang.

Bolsover, G., 1948. Soviet Ideology and Propaganda. *International Affairs*, 24(2), pp. 170–180.

Braghiroli, S., Makarychev, A., 2017. Redefining Europe: Russia and the 2015 Refugee Crisis. *Geopolitics*, 23(4), pp. 823–848.

Brandenberger, D., 2011. *Propaganda State in Crisis: Soviet Ideology, Indoctrination, and Terror under Stalin, 1927-1941.* Yale University Press.

Bruusgaard, K., 2014. Crimea and Russia's Strategic Overhaul. *Parameters*, 44(3), pp. 81–90.

Brzezinski, Z., 1960. Communist Ideology and International Affairs. *Journal of Conflict Resolution*, 4(3), pp. 266–291.

Buecker, R., 2003. Karl Marx's Conception of International Relations. *Glendon Journals of International Relations*, 3, pp. 49–58.

Bugajski, J., 2020. *The Balkan Great Game*. CEPA - Center for European Policy Analysis. [Online source] Available from: https://www.cepa.org/the-great-balkan-game [Accessed 09.04.2020].

Burlinova, N., 2015. Russian Soft Power is Just Like Western Soft Power, but with a Twist. *Russia Direct*. [Online source] Available from: https://russia-direct.org/opinion/russian-soft-power-just-western-soft-power-twist [Accessed 17.02.2020].

Carey, A., 1996. *Taking the Risk Out of Democracy: Corporate Propaganda versus Freedom and Liberty (History of Communication)*. University of Illinois Press.

Carpenter, M., 2017. *Fighting in the 'Grey Zone': Lessons from Russian Influence Operations in Ukraine*. Biden Center for Diplomacy and Global Engagement.

Cassinelli, C., 1960. Totalitarianism, Ideology, and Propaganda. *The Journal of Politics*, 22(1), pp. 68–95.

Chebankova, E., 2015. Contemporary Russian Conservatism. *Post-Soviet Affairs*, 32(1), pp. 28–54.

CIA - Office of Soviet Analysis, 1955. *Communist Psychological Warfare in the Framework of the Cold War*. General CIA Records. USA - Central Intelligence Agency. [Online source] Available from: https://www.cia.gov/library/readingroom/document/cia-rdp83-00418r004400080006-8 [Accessed 26.01.2020].

Cimbala, S., 2014. Sun Tzu and Salami Tactics? Vladimir Putin and Military Persuasion in Ukraine. *The Journal of Slavic Military Studies*, 27(3), pp. 359–379.

Cockrell, C., 2017. Russian Actions and Methods against the United States and NATO. *Military Online Exclusive*. [Online source] Available from: https://www.armyupress.army.mil/Portals/7/Army-Press-Online-Journal/documents/Cockrell-v2.pdf [Accessed 07.12.2019].

Cull, N., *et al.*, 2017. *Soviet Subversion, Disinformation and Propaganda: How the West Fought Against it*. The London School of Economics and Political Sciences - Institute of Global Affairs.

Darczewska, J., 2014. The anatomy of Russian information warfare: The Crimean operation, a case study. *Point of View*, 42, pp. 1–37.

Diesen, G., 2019. Russia as an international conservative power: the rise of the right-wing populists and their affinity towards Russia. *Journal of Contemporary European Studies*, 28(2), pp. 182-196.

Dimitrova, A., *et al.*, 2017. *The Elements of Russia's Soft Power: Channels, Tools, and Actors Promoting Russian Influence in the Eastern Partnership Countries*. Working Paper No. 4. EU-STRAT.

Doob, L., 1949. The Strategies of Psychological Warfare. *The Public Opinion Quarterly*, 13(4), pp. 635–644.

Doroszczyk, J., 2018. Russian Active Measures in Psychological Warfare. *Polish Political science Yearbook*, 47(3), pp. 521–534.

Ellehuus, R., 2020. *Mind the Gaps: Russian Information Manipulation in the United Kingdom*. CSIS - Center for Strategic and International Studies. [Online source] Available from: https://www.csis.org/analysis/mind-gaps-russian-information-manipulation-united-kingdom [Accessed 09.04.2020]

Ermus, A., Salum, K., 2016. Changing Concepts of War: Russia's New Military Doctrine and the Concept of Hybrid Warfare. In *Russian Information Campaign Against the Ukrainian State and Defence Forces* (Sazonov, V., Müür, K., Mölder, H. ed.), pp. 53-60. NATO Strategic Communications Centre of Excellence.

Fedchenko, Y., 2016. Kremlin Propaganda: Soviet Active Measures by Other Means. *Estonian Journal of Military Studies*, 2, pp. 141–170.

Fedyk, N., 2017. Russian "New Generation" Warfare: Theory, Practice, and Lessons for U.S. Strategists. *Small Wars Journal*. [Online source] Available from: https://smallwarsjournal.com/jrnl/art/russian-"new-generation"-warfare-theory-practice-and-lessons-for-us-strategists-0 [Accessed 04.11.2018].

Feklyunina, V., 2016. Soft power and identity: Russia, Ukraine and the "Russian world(s)". *European Journal of International Relations*, 22(4), pp. 773–796.

Finch, L., 2000. Psychological Propaganda: The War of Ideas on Ideas During the First Half of the Twentieth Century. *Armed Forces & Society*, 26(3), pp. 367–386.

Flemming, H., 2017. *Russian Hybrid Warfare: A Study of Disinformation*. DIIS - Danish Institute for International Studies.

Franke, U., 2015. *War by non-military means Understanding Russian information warfare*. FOI - Swedish Defence Research Agency.

Freedman, D., 2015. Paradigms of Media Power. *Communication, Culture & Critique*, 8(2), p. 273-289.

Giles, K., 2016a. *Handbook of Russian Information Warfare*. NATO Defense College.

Giles, K., 2016b. *The Next Phase of Russian Information Warfare*. NATO Strategic Communications Centre of Excellence.

Giles, K., Sherr, J., Seaboyer, A., 2018. *Russian Reflexive Control*. Royal Military College of Canada.

Hellman, M., Wagnsson, C., 2017. How can European states respond to Russian information warfare? An analytical framework. *European Security*, 26(2), pp. 153–170.

Hinck, R., Kluver, R., Cooley, S., 2018. Russia re-envisions the world: strategic narratives in Russian broadcast and news media during 2015. *Russian Journal of Communication*, 10(1), pp. 21–37.

Hofmeisterová, P., *et al.*, 2018. *Характеристика прокремловской пропганды в центральной и восточной Европе и примеры как с ней справиться*. NESEHNUTÍ – NEzávislé Sociálně Ekologické HNUTÍ.

Hudson, V., 2013. *A Study of the Civilisational Aspects of Russian Soft Power in Contemporary Ukraine*. Doctoral Thesis. University of Birmingham.

Isar, Y., 2017. Cultural Diplomacy: India Does It Differently. *International Journal of Cultural Policy*, 23(6), pp. 705–716.

Jang, K., 2019. Between Soft Power and Propaganda: The Korean Military Drama Descendants of the Sun. *Journal of War & Culture Studies*, 12(1), pp. 24–36.

Jowett, G., O'Donnell, V., 2012. *Propaganda and Persuasion, 5th ed.* SAGE Publications.

Karaganov, S., 2018. The new Cold War and the emerging Greater Eurasia. *Journal of Eurasian Studies*, 9(2), pp. 85–93.

Keating, V., Kaczmarska, K., 2019. Conservative Soft Power: Liberal Soft Power Bias and the "Hidden" Attraction of Russia. *Journal of International Relations and Development*, 22(1), pp. 1–27.

Klyueva, A., 2017. *Strategic Narratives of Public Diplomacy and the Enhancement of Soft Power: An Exploratory Study*. Doctoral Thesis. University of Oklahoma.

Klyueva, A., Mikhaylova, A., 2017. Building the Russian World: Cultural Diplomacy of the Russian Language and Cultural Identity. *JOMEC - Journalism, Media and Cultural Studies*, 11, pp. 127–143.

Kortunov, A., 2019. *Between Polycentrism and Bipolarity: On Russia's World Order Evolution Narratives*. Russia in Global Affairs.

Krenn, M., 2017. *The History of United States Cultural Diplomacy: 1770 to the President Day*. Bloomsbury Academic.

Kuusinen, O., *et al.*, 1963. *Fundamentals of Marxism and Leninism, 2nd Revisited Edition*. Foreign Languages Publishing House, Moscow.

Kuzio, T., 2019. Old Wine in a New Bottle: Russia's Modernization of Traditional Soviet Information Warfare and Active Policies Against Ukraine and Ukrainians. *The Journal of Slavic Military Studies*, 32(4), pp. 485–506.

Lammi, W., 1997. The Hermeneutics of Ideological Indoctrination. *Perspectives on Political Science*, 26(1), pp. 10–14.

Lanoszka, A., 2016. Russian Hybrid Warfare and Extended Deterrence in Eastern Europe. *International Affairs*, 92(1), pp. 175–195.

Laruelle, M., 2015a. *The "Russian World". Russia's Soft Power and Geopolitical Imagination*. CGI - Center on Global Interests.

Laruelle, M., 2015b. Russia as a "Divided Nation". From Compatriots to Crimea: A Contribution to the Discussion on Nationalism and Foreign Policy. *Problems of Post-Communism*, 62(2), pp. 88–97.

Lenczowski, J., 2009. Cultural Diplomacy, Political Influence & Integrated Strategy. In *Strategic Influence: Public Diplomacy, Counterpropaganda and Political Warfare* (Waller, M., ed.), pp. 74-99. Crossbow Press.

Light, M., 1991. Soviet Policy in the Third World. *International Affairs*, 67(2), pp. 263–280.

Liu, X., 2019. China's Cultural Diplomacy: A Great Leap Outward with Chinese Characteristics? Multiple Comparative Case Studies of the Confucius Institutes. *Journal of Contemporary China*, 28(118), pp. 646–661.

Lord, C., 2009. Public Diplomacy and Soft Power. In *Strategic Influence, Public Diplomacy, Counterpropaganda And Political Warfare* (Waller, M., ed.), pp. 61-73. Crossbow Press.

Lucas, E., Nimmo, B., 2015. *Information Warfare: What Is It and How to Win It?*. CEPA - Center for European Policy Analysis.

Lucas, E., Pomerantsev, P., 2016. *Winning the Information War. Techniques and Counter-strategies to Russian Propaganda in Central and Eastern Europe*. CEPA - Center for European Policy Analysis.

Lukin, A., 2014. Eurasian Integration and the Clash of Values. *Survival: Global Politics and Strategy*, 56(3), pp. 43–60.

Mankoff, J., 2020. *Russian Influence Operations in Germany and Their Effect*. CSIS - Center for Strategic and International Studies. [Online source] Available from: https://www.csis.org/analysis/russian-influence-operations-germany-and-their-effect [Accessed 13.05.2020]

Meister, S., 2016. *Isolation and Propaganda: The Roots and Instruments of Russia's Disinformation Campaign*. Transatlantic Academy.

Meister, S., (ed.) 2018. *Understanding Russian Communication Strategy: Case Studies of Serbia and Estonia*. Edition Culture and Foreign Policy. IFA - Institut für Auslandsbeziehungen.

Melissen, J., 2005. *The New Public Diplomacy Soft Power in International Relations*. Palgrave McMillan.

Merrill, J., Lowenstein, R., 1971. *Media, messages, and men; new perspectives in communication*. D. McKay Co.

Mintzberg, H., *et al.*, 2002. *Strategy Process: Concepts, Context, Cases, 4th ed.* Prentice Hall.

Miskimmon, A., O'Loughlin, B., 2017. Russia's Narratives of Global Order: Great Power Legacies in a Polycentric World. *Politics and Governance*, 5(3), pp. 111–120.

Mölder, H., Sazonov, V., 2018. Information Warfare as the Hobbesian Concept of Modern Times – Principles, Techniques and Tools of Russian Information Operations in Donbas. *The Journal of Slavic Military Studies*, 31(3), pp. 308–328.

Nietzel, B., 2016. Propaganda, Psychological Warfare and Communication Research in the USA and the Soviet Union during the Cold War. *History of the Human Sciences*, 29(4–5), pp. 59–76.

Nissen, T., 2015. *The Weaponization Of Social Media*. Royal Danish Defence College.

Papp, D., 1979. Toward an Estimate of the Soviet Worldview. *Naval War College Review*, 32(7), pp. 60–77.

Partanen-Dufour, R., 2016. *How Russia Today supported the annexation of Crimea; A Study of the Media's role in Hybrid Warfare*. Independent thesis. Uppsala University.

Pasitselska, O., 2017. Ukrainian crisis through the lens of Russian media: Construction of ideological discourse. *Discourse & Communication*, 11(6), pp. 591–609.

Pechatnov, V., 2001. Exercise in Frustration: Soviet Foreign Propaganda in the Early Cold War, 1945-47. *Cold War History*, 1(2), pp. 1–27.

Perry, B., 2015. Non-linear Warfare in Ukraine: The Critical Role of Information Operations and Special Operations. *Small Wars Journal*. [Online source] Available from: https://smallwarsjournal.com/jrnl/art/non-linear-warfare-in-ukraine-the-critical-role-of-information-operations-and-special-opera [Accessed 23.02.2020]

Pomerantsev, P., Weiss, M., 2014. *The Menace of Unreality: How the Kremlin Weaponizes Information, Culture and Money*. The Institute of Modern Russia.

Pynnöniemi, K., 2018. Russia's National Security Strategy: Analysis of Conceptual Evolution. *Journal of Slavic Military Studies*, 31(2), pp. 240–256.

Pynnöniemi, K., Rácz, A., 2016. *Fog of Falsehood: Russian Strategy of Deception and the Conflict in Ukraine*. FIIA - The Finnish Institute of International Affairs.

Qualter, T., 1962. *Propaganda and Psychological Warfare*. Random House.

Rotărescu, C., 2015. Ukrainian Hybrid War – Quo Vadis?. *Scientific Bulletin*, 20(1), pp. 151–159.

Rotaru, V., 2017. Forced Attraction? How Russia is Instrumentalizing Its Soft Power Sources in the "Near Abroad". *Problems of Post-Communism*, 65(1), pp. 1–12.

Rutenberg, J., 2017. RT, Sputnik and Russia's New Theory of War: How the Kremlin built one of the most powerful information weapons of the 21st century — and why it may be impossible to stop. *The New York Times Magazine*. [Online source] Available from: https://www.nytimes.com/2017/09/13/magazine/rt-sputnik-and-russias-new-theory-of-war.html [Accessed 11.08.2018].

Rutland, P., Kazantsev, A., 2016. The Limits of Russia's "Soft Power". *Journal of Political Power*, 9(3), pp. 395–413.

Schweitzer, A., 1962. Ideological Strategy. *The Western Political Quarterly*, 15(1), pp. 46–66.

Sergunin, A., and Karabeshkin, L., 2015. Understanding Russia's Soft Power Strategy. *Politics*, 35(3–4), pp. 347–363.

Shcherbak, A., 2019. *When Conservatism and Nationalism Form the Spurs of Kremlin Ideology*. Policy Memo No. 609. PONARS Eurasia.

Simons, G., 2013. *Nation Branding and Russian Foreign Policy*. The Swedish Institute of International Affairs.

Simons, G., 2014. Russian Public Diplomacy in the 21st Century: Structure, Means and Message. *Public Relations Review*, 40(3), pp. 440–449.

Smith, C., 1953. Psychological Warfare. *Naval War College Review*, 6(2), pp. 39–61.

Snegovaya, M., 2015. *Putin's Information Warfare in Ukraine: Soviet Origins of Russia's Hybrid Warfare*. Institute for the Study of War.

Sproule, M., Lewis, W., 1994. *Channels of Propaganda*. Grayson Bernard Pub.

Staar, R., 1991. *Foreign Policies of the Soviet Union*. Hoover Press Publication.

Stefanov, R., Vladimirov, M., 2018. Russian influence on the media: a case study of Serbia. In *Understanding Russian Communication Strategy: Case Studies of Serbia and Estonia* (Meister, S., ed.), pp. 15-39. IFA - Institut für Auslandsbeziehungen.

Stronski, P., Sokolsky, R., 2020. Multipolarity in Practice: Understanding Russia's Engagement With Regional Institutions. *Carnegie Endowment for International Peace*. [Online source] Available from: https://carnegieendowment.org/2020/01/08/multipolarity-in-practice-understanding-russia-s-engagement-with-regional-institutions-pub-80717 [Accessed 08.03.2020].

Suslov, M., 2017. *Russian World: Russia's Policy Towards its Diaspora*. Russie. Nie.Visions. Institut Francais des Relations Internationales.

Szostek, J., 2017. Nothing Is True? The Credibility of News and Conflicting Narratives during "Information War" in Ukraine. *The International Journal of Press/Politics*, 23(1), pp. 116–135.

Thomas, T., 2016. The Evolution of Russian Military Thought: Integrating Hybrid, New-Generation, and New-Type Thinking. *The Journal of Slavic Military Studies*, 29(4), pp. 554–575.

Thompson, T., 1989. *Ideology and Policy: The Political Uses of Doctrine in The Soviet Union*. Routledge.

Tiido, A., 2015. The Russian World: The Blurred Notion of Protecting Russians Abroad. *Polski Przegląd Stosunków Międzynarodowych*, 5, pp. 131–151.

Tolz, V., Teper, Y., 2018. Broadcasting agitainment: a new media strategy of Putin's third presidency. *Post-Soviet Affairs*, 34(4), pp. 213–227.

Triska, J., 1958. A Model for Study of Soviet Foreign Policy. *The American Political Science Review*, 52(1), pp. 64–83.

Watson, I., 2012. South Korea's State-led Soft Power Strategies: Limits on Inter-Korean Relations. *Asian Journal of Political Science*, 20(3), pp. 304–325.

White, J., 2016. *Dismiss, Distort, Distract, and Dismay: Continuity and Change in Russian Disinformation*. Report No.13. IES - Institute for European Studies.

Wilson, J., 2015. Soft Power: A Comparison of Discourse and Practice in Russia and China. *Europe-Asia Studies*, 67(8), pp. 1171–1202.

Yablokov, Y., 2015. Conspiracy Theories as a Russian Public Diplomacy Tool: The Case of Russia Today (RT). *Politics*, 35(3–4), pp. 301–315.

Zamorano, M., 2016. Reframing Cultural Diplomacy: The Instrumentalization of Culture under the Soft Power Theory. *Culture Unbound*, 8, pp. 166–186.

Zeleneva, I., Ageeva, V., 2017. Russia's soft power in the Baltics: media, education and Russian world narrarive. *Media Education*, 4, pp. 181–188.

Zevelev, I., 2001. *Russia and Its New Diasporas*. United States Institute of Peace.

Zimmerman, W., 1969. *Soviet Perspectives on International Relations, 1956-1967*. Princeton University Press.

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. *Babak 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*

2019

The Obstacles and Enablers of US-EU Counter-Terrorism Cooperation: The Case of the Passenger Name Record. *Rain Alev*

Baltic States and the Zapad 2017 Exercise in the Western Media: Implications for Small State Strategic Communication. *Kerli Onno*

Cybersecurity Education in Estonia: Building Competences for Internal Security Personnel. *Piret Pernik*

Work, Prey, Love: A Critical Analysis of Estonian Cybercrime Case Law 2014-2019. *Kristjan Kikerpill*

Development and Prevention of Juvenile Fire-related Risk Behaviour in the Social Learning Process. *Margo Klaos, Diva Eensoo, Kadi Luht-Kallas, Jaanika Piksööt*

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*

Inspectors Of The Environmental Inspectorate Confused With The Right To Apply Direct Coercion. *Ülle Vanaisak*

Clarifying (Wicked) Safety Problems With a Network Analysis Tool. *Priit Suve*

EDITORIAL POLICY AND DISCLAIMER

The Proceedings of the Estonian Academy of Security Sciences is a non-profit academic journal that publishes well-documented and analysed studies on a full range of contemporary security issues, especially internal security and law enforcement.

Priority is given to the more recent dimensions of international security and risk management developments and innovations, including original case studies, the rise of global security challenges and future perspectives.

The Proceedings considers manuscripts on the following conditions:

- The submitted manuscript is an original work in the field and does not duplicate any other previously published work.
- The manuscript has been submitted only to the Proceedings and is not under consideration for peer-review or has not been accepted for any other publication at the same time, and has not already been published elsewhere.
- The manuscript contains nothing that is morally binding, discriminating or illegal.

By submitting your manuscript you are also agreeing to the necessary originality checks your work may have to undergo during the peer-review, editorial and publishing processes.

All reasonable claims to co-authorship must be clearly named in the manuscript. The corresponding author must be authorised by all co-authors to act on their behalf in all matters pertaining to the publication process. The order of names should also be agreed upon in advance of submission by all authors. The Author must follow the **Harvard style of referencing** and supply all details required by any funding and grant-awarding bodies if appropriate. Authors must also incorporate a statement which will acknowledge any financial interest or benefit they have arising from the direct applications of their submitted study. For all manuscripts a non-discriminatory approach in language usage is mandatory. When using wording which has been or is asserted to be a proprietary term or trademark, the Author must use the symbol ® or TM. There is no submission fee for Proceedings. Fees for Author(s) are exceptional and an object for separate negotiations and agreements. If you wish to include any material in which you do not hold copyright, you must obtain written permission from the copyright owner prior to manuscript submission.

GENERAL REQUIREMENTS FOR THE MANUSCRIPTS

Manuscripts for publication should be submitted in academic English. The Editorial Team accepts Estonian language articles of exceptionally high quality and provides translation to English.

A manuscript should not exceed the limit of 45 000 characters (with spaces). The material in the manuscript should be presented in the following order:

- The full title of the manuscript;
- The name and surname of the author(s), the scientific degree and title, the name of the institution, position, address, phone and e-mail;
- Abstract (500-600 characters);
- The key words (3-5 words);
- The text of the manuscript;
- The list of references (in alphabetical order).

The manuscript should be submitted with single line spacing, normal margins, font type Times New Roman size 12. Justified text alignment is used and paragraphs are separated by a free line or extra spacing.

All headings, except introduction and conclusion, are numbered with Arabic numbers by subdivisions (1., 1.1., 1.1.1). There is no need to start each chapter from a new page or insert superfluous free lines, this will be done by the editor. All tables, figures and pictures used in the article are presented in a separate file with a high resolution (preferably .jpg, .gif or .pdf format). The scanned images should not be less than 600 dpi, and pictures downloaded from the web should not be less than 100KB in size. A reference is provided in the text as to where the table is supposed to be located.

The Editor reserves the right to abridge and edit submitted texts, as well as to change their titles.

Articles can be submitted throughout the year. However the term of submission of the articles to be published during a given year is the **31st of May.**
The manuscript shall be submitted electronically in .rtf or word format to teadusinfo@sisekaitse.ee.

The publisher reserves the rights to reject or return the manuscripts that do not satisfy the above requirements.

PEER-REVIEW PROCESS

The Proceedings operates on an academic quality policy of double-blind international peer-review. This means that the identity of authors and reviewers are closed during the process.

Submitted manuscripts will be sent to the Editorial Board and then to two or more peer-reviewers, unless the manuscripts are considered to either be lacking in presentation or the written English is below an academic level.

Submitted manuscripts which are not deemed to be out of scope or below the threshold for the journal will be reviewed by two academic experts. Statistical or other relevant topically specialised reviewers are also used where needed. Reviewers are asked to express their competing interests and have to agree to peer-review. Reviewers are asked whether the manuscript is academically competent and coherent, how relevant and important it is and whether the academic quality of the writing is acceptable, as well as suggestions for further revision and improvement of a submitted manuscript.

The final decision is made on the basis that the peer-reviewers are in accordance with one another, or that at least there are no bold dissenting positions. At least one peer-review should be positive in total for the final positive decision. In cases where there is strong disagreement either among peer-reviewers or between the author and peer-reviewers, additional advice is sought from members of the Editorial Board. Additional editorial or external peer-review is also requested when needed. The Proceedings normally allows two revisions of any submitted and peer-reviewed manuscript.

All appeals and claims should be directed to the Editors. The ultimate responsibility for editorial decisions and academic quality lies with the Editorial Board and the Editor-in-Chief.

Reasoned misunderstandings and claims are subject to additional assessment by the Editorial Board in accordance with academic traditions or relevant law.

SISEKAITSEAKADEEMIA
ESTONIAN ACADEMY OF SECURITY SCIENCES

JOURNAL CAN BE VIEWED ONLINE
IF YOU WOULD LIKE TO SEE THE FIGURES AND PICTURES IN COLOUR

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

ISBN 978-9985-67-333-1 (print)
ISBN 978-9985-67-334-8 (pdf)