SISEKAITSEAKADEEMIA
ESTONIAN ACADEMY OF SECURITY SCIENCES

Internal Security Institute

ERKKI KOORT, INGE LINDSAAR,
MARIITA MATTIISEN, TRIIN PIIP

HYBRID THREATS AND THEIR IMPACT ON EUROPEAN SECURITY

SEMINAR SUMMARY

HYBRID THREATS AND THEIR IMPACT ON EUROPEAN SECURITY

SEMINAR SUMMARY

COMPILERS: ERKKI KOORT, INGE LINDSAAR, MARIITA MATTIISEN, TRIIN PIIP

SISEKAITSEAKADEEMIA
ESTONIAN ACADEMY OF SECURITY SCIENCES

Front cover image: Shutterstock

Layout: Jan Garshnek

ISBN: 978-9985-67-352-2

www.sisekaitse.ee/kirjastus

CONTENTS

INTRODUCTION

Hybrid threats are nothing new and, according to some experts, **have been used for centuries**. Hybrid threats are highlighted in the EU Security Union Strategy 2020-2025, which defines hybrid threats as **a mixture of coercive and subversive practices, combining traditional and non-traditional methods (i.e. diplomatic, military, economic, technological) that can be used in a coordinated way by national or non-state actors to achieve specific objectives, however, below the officially declared threshold of warfare**[1].

Hybrid threats have not only come to stay, but they are constantly evolving. On the one hand, their manifestation and extent are difficult to predict, and on the other hand, there is reason to believe that the frequency of hybrid attacks will increase. Today, hybrid measures are closely linked to technology, which makes them even more difficult to detect and fight. However, we cannot forget that there is a human being behind every hybrid threat and its implementation.

Although the methods of hybrid warfare are evolving and changing, the methods that have proved effective remain. Hybrid attacks affect and can paralyze society or individual parts of it, either at national level or regionally. There is a broad understanding in the European Union of what we are facing in the form of hybrid threats. Awareness of hybrid threats and the development of resilience are constantly being developed, both in the EU institutions and in cooperation with various partners. Fortunately, there is more common language and mutual understanding in this area than ever before.[2] However, it covers a high political level, but **does not cover all areas of hybrid threats and needs to be disseminated more widely, based on knowledge.**

Educating people, including in the fight against hybrid threats, is the key. Officials and decision-makers, as well as businesses, senior executives and the public who are aware of and understand the threats, are our strengths and improve our resilience to hybrid threats. Although we know what hybrid threats are, and hopefully will recognize them when they arise, there is a need for a common knowledge-based response to hybrid threats.

The mentioned fact was also one of the reasons why **Internal Security Institute of the Estonian Academy of Security Sciences, in a close cooperation with the Intelligence**

---

1 Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions on the EU Security Union Strategy Brussels, 24.7.2020 [www] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0605 (last visit 7.10.2021)

2 EU Commission president accuses Belarus of launching 'hybrid attack' against Europe, 15.09.2021 [www] https://www.aa.com.tr/en/europe/eu-commission-president-accuses-belarus-of-launching-hybrid-attack-against-europe/2365349 (last visit 7.10.2021)

College in Europe, held a web-based seminar on hybrid threats and their impact on European security in Tallinn, Estonia, on 16–17 June 2021.

At the event, many distinguished speakers from Estonia, Ukraine, Finland, UK, US, Canada, and EU were represented, covering different angles of hybrid threats and their methods. The target group of the event were leaders and senior officials of European security and intelligence services, law enforcement authorities, representatives of respective ministries, and educational institutions. **The seminar gave the audience an overview of hybrid threats from the perspective of politicians, policy makers, researchers, and practitioners**. It also provided the audience with an opportunity to ask questions from globally recognized experts on the subject matter as well as high-level practitioners with extensive experience in the field.

KEY POINTS OF THE SEMINAR

- Hybrid warfare is **weaponization of everything** that includes and affects the whole society and all its sectors, with the aim of creating chaos.
- The goal of the hybrid warfare is to influence the targeted country's society **to change its decisions and course** to the desired direction, or to prepare the society for possible intervention in the future.
- The goal for Russia is **to create the Soviet Union 2.0 and re-establish the sphere of influence** in their neighbouring countries to once again become a global power.
- In the toolbox of Russian hybrid warfare, **intelligence services and media outlets** play a crucial role.
- Hybrid warfare methods **develop and change constantly**. Those proven to be successful remain.
- Stronger together: **the EU and NATO should work together** in combating hybrid warfare. The more like-minded allies and partners we have, the stronger we are.
- **Educating our people** is the key. Population who is aware and understands and recognizes threats is our strength and improves our resilience.
- **Situational awareness and early warning** are crucial. This means both awareness of threats and courage to make decisions by the political leadership and the overall up-to-date situational awareness by experts dealing with the topic on the daily basis. Early warning, as in every other war-related situation, is crucial to increase resilience and prepare a counterattack on time.
- **Attribution of the hybrid attacks** is difficult but crucial in countering and deterring hybrid threats.
- Russian state-controlled media channels **are not media but proxies** and should be treated as such.

OVERVIEW

As mentioned before, hybrid threats are nothing new and, based on some opinions, have been used for centuries. However, hybrid threats have developed and will continue to develop: the so-called toolbox of hybrid measures is replenishing constantly. When some elements of hybrid warfare, such as information warfare, were actively used already during the Cold War or even earlier, cyber elements have been added to the *modus operandi* no more than a few decades ago. Even though we know what hybrid threats are and, hopefully, recognize them when they occur, there is still no official definition of the phenomenon. Some experts have defined hybrid threats as follows:

"Hybrid warfare is an instrument and a form of multidimensional warfare where the measures of unrestricted coercive force are expanded and combined on a wide spectrum of inter-human interaction to make the opponent's ways to sustain, perceive and defend itself obsolete." (Keir Giles in: Giles, Keir/Seaboyer, Anthony (2020): Russia in the Grey Zone, DRDC.);

others as such:

"Hybrid threats refer to a wide range of methods or activities used by hostile state or non-state actors in a coordinated manner in order to target the vulnerabilities of democratic states and institutions, while remaining below the threshold of formally declared warfare. Some examples include cyber-attacks, election interference and disinformation campaigns, including on social media." (Council Press Release 2019)

Hybrid warfare is mainly used by the Russian Federation (RF), People's Republic of China, Islamic Republic of Iran, and Democratic People's Republic of Korea (North Korea), but also by armed non-state actors. As the RF has been the main actor towards the West, the seminar concentrated mostly on discussing the actions and methods used by the RF.

The toolbox of hybrid measures, to name a few, includes psychological warfare, propaganda, disinformation campaigns, cyberattacks, lawfare, conspiracy theories, apolitical parties, resistance groups, covert actions, rewriting history, etc., which are used simultaneously with the main goal to create chaos in a targeted country. Some of the well-known examples also pointed out by the speakers during the seminar were the Bronze Soldier crisis (including massive cyberattacks) in Estonia in 2007, the attack on Georgia in 2008, and the annexation of the Crimea in 2014 – all of them initiated and conducted by the RF. Even though hybrid actions are generally not conducted by militaries, but mostly by security services, intelligence services, or different individuals, it can also include elements of kinetic warfare. It is also a question of how to distinguish between such actors. Some Russian special services are part of the armed forces, some of them will be part of the army during an armed conflict, and most of them have military

structure. Different individuals might also act in the name of the state or wish to copy state activities, as they understand them. Considering the above, hybrid warfare can be said to be "a weaponization of everything" where the vulnerabilities of targets are used for an attack. Nowadays, hybrid actions are closely connected to technology, which makes them even harder to detect and counter.

But, in the end, there is still a person behind all of that, may it be the one actually conducting the attacks or the one giving the orders to do so. When we can attribute an attack to a specific individual and to a country it represents, it makes it also easier to counter and deter the threat itself. The annexation of the Crimea and war in Eastern Ukraine is an example here once again. During the first weeks of the attack, there was no information about who were those little green men, and it was therefore not possible to take any further steps. As soon as they were attributed to the RF, measures, for example, sanctions, became possible to implement.

The *modus operandi* of hybrid warfare is as complex as the term itself. As mentioned earlier, it covers the whole society and uses whatever means to achieve the attacker's goal. For the most part, the goal is to change the targeted country's decisions via interfering in its internal affairs and/or preparing the targeted country's population to support the forthcoming intervention (for example, the Crimean status referendum). Methods to achieve this are different and generally used simultaneously. When cyberattacks, customs restrictions, political pressure or fake news can be considered as direct hybrid attacks, there are also more hidden methods that may not even look like hybrid warfare methods in the first place. To mention some, these can be the use of GONGOS[3], local influence agents, soft power movies, music videos or books, children's summer camps, university scholarships, Russian international TV and other media channels, etc. The methods RF is using in its hybrid operations are not new and originate largely from the Soviet times, or more precisely, from the KGB[4] "workbook".

When it comes to hybrid warfare, intelligence services and media companies are listed as major tools in RF hybrid warfare operations.

Intelligence services as one of the key tools is not only used for target killings or covert operations. Intelligence services also play a crucial role in planning and conducting different hybrid attacks. Already during the Cold War, 85% of the KGB's work concerned information or psychological operations (the so called *active measures* or "активные мероприятия" in Russian), while only 15% of its work was related to espionage and intelligence. This mindset has not changed, and the KGB methods are still in use, while all modern RF intelligence agencies have their role in the hybrid warfare. For example, the SVR[5], operating mostly abroad, has like-minded journalists and think-tankers in the host country to help them reproduce the Kremlin's narratives. While the GRU[6] has been involved in the high visibility violent operations, it also has good online capabilities, for example, their own troll outlets, covert media outlets, etc.

Russian state-controlled media outlets, which applies to most of the media outlets in RF, have been and continue to be another key tool in hybrid warfare tactics. Directed from the Kremlin, state-controlled media outlets have the control over narratives and topics and are, therefore, a powerful tool for the authorities to control the media sphere and spread their narratives abroad. This gives the Kremlin the ability to control their own

[3] GONGO – Government-Organised Non-Governmental Organisations
[4] KGB – Committee for State Security of the Soviet Union (1954–1991)
[5] SVR – Foreign Intelligence Service of the Russian Federation
[6] GRU – Military Intelligence of the Russian Federation

population and influence the public opinion in the population of the targeted countries. Therefore, Russian media channels are not the media. They are proxies and should be treated as such.

Another hybrid warfare tool widely used by the RF already since the 17th century is lawfare, which basically means justifying and legalizing its actions through referring to the international law. The RF uses principles of the international law based on its self-interest. To paraphrase Alexander Wendt, "International law is what states make of it". The use of lawfare is not restricted to Ukraine or Georgia only, where the justification refers to the nation's ethnic self-determination principle (the referendum in the Crimea) or to the right to protect Russians abroad, but is actively used also in the Arctic, claiming part of the territory to be historically Russian. Claiming that the RF works in the framework of the international law makes the RF's actions legal, at least in the eyes of their own people.

Even though hybrid warfare methods develop and change, the ones that have proven to be efficient remain. To conclude, the RF does not usually care as to which methods from the hybrid toolbox to use, as long as they serve the goal. **For example, during the COVID-19 crisis, the topic has been skilfully used in the RF propaganda narratives and conspiracy theories to showcase Russia as a hero** (for instance, aid to Italy, where they used the label "From Russia with love") and the West as failed in dealing with the crisis. Nowadays, the goal of using hybrid warfare methods is rather destabilization of others than presenting a competitive political agenda, like it used to be the case during the Soviet times.

RECOMMENDATIONS SUGGESTED THE SPEAKERS

When it comes to **countering hybrid threats, the West has been slow and showed the lack of initiative**, which has made its actions rather reflective. NATO-EU joint declarations, the EU INCEN hybrid cell, cooperation between member states and also the work of private companies (for instance, Bellingcat) and individuals (for instance, Jessikka Aro) shows that the West has now understood what it is facing and is constantly developing its awareness and resilience inside the institutions and also with different partners. Consequently, there are almost no disagreements inside the EU anymore when it comes to hybrid threats. **There is more common ground and mutual understanding in this field than ever before**. However, it does not cover all areas of hybrid threats. For example, the EU has not been very active in taking steps to deal with the Russian state-controlled media channels. There should also be common understanding that these channels do not serve the free media but the narratives and goals of the Russian state. Ukraine has been more concrete here, banning Russian social media channels in 2017 and sanctioning three Kremlin-linked TV channels in 2021. Some steps have also been taken against the Russian media channels in the Baltics. However, to counter Russian state-controlled media successfully, the EU should be more united in that, too.

To counter hybrid warfare efficiently, early warning and situational awareness are also one of the key elements. Early warning, as in every other war-related situation, is crucial to increase resilience and prepare the counterattack on time. The West should cooperate internally and also externally with the like-minded partners to create a better situational awareness among the authorities and also among the population. The population needs to be aware of the situation, since educated population is the key for building resilience and strength. Working together with governments, NGOs, the media and other actors makes the West more united and, therefore, better prepared to counter the hybrid threats we are facing today.

Internal Security Institute of the Estonian Academy of Security Sciences **recommends continuing with joint conferences, seminars, and meetings on hybrid threats**. This will allow finding common ground and share experiences that are not covered with different levels of classification. Internal Security Institute recommends discussing during the forthcoming meetings **whether the EU members should need hybrid defence strategies**. Also, academic discussion allows elaborating on the hypothesis about the **necessity of hybrid attack strategies**.

SHORT BIOGRAPHIES OF SPEAKERS

DAY 1

Erkki Koort

Erkki Koort is the Head of Internal Security Institute in Estonian Academy of Security Sciences since 2018. He is responsible for the development of Internal Security Institute and for the development of scientific researches in the Academy of Security Sciences. Institute is the body implementing and coordinating Internal Security Master Studies in Estonia and in its' partners master programmes in FRONTEX and in CEPOL.

Erkki Koort has an extensive experience as Deputy Secretary General for Internal Security Policy covering the whole spectrum of internal security- Border Management, Law Enforcement, Migration and Rescue Policy and the EU Funds during 2007-2018 in Estonian Ministry of the Interior. He was responsible for the development of internal security policy, strategic planning, coordination of legislative and regulatory drafting and for strategic risk-analyses in the Internal Security Policy department and Foreign Financing Department of the Ministry. His recent responsibilities covered also strategic guidance and supervising the agencies' activities in the field of internal security, border control, counterterrorism, criminal police and anti-corruption. In addition, Erkki was responsible for the coordination of the European and international affairs of the Ministry, as well as for implementation of relevant EU- funded projects, communication and inter-institutional relations in the field of internal security. He was one of the main spoke persons of the Ministry.

Mr Koort is also known as the Head of the Estonian delegation to Standing Committee on Operational Cooperation on Internal Security (COSI) and as the Head of the Estonian Counter-terrorism Council.

During 2008-2018 Erkki was the Chairman of Estonian Forensic Science Institute Council where he was managing the strategic development of the Estonian Forensic Science Institute. The Estonian Forensic Science Institute is considered today as one of the most modern and innovative forensic institutions in Europe.

In 2011, Mr Koort was the member of Estonian Internet Foundation Council supervising the strategic development of the foundation and coordinating the development and innovation in the area. The Estonian Internet Foundation represents the Estonian Internet Community and handles the management of Estonia's top-level *domain.ee* and its sub-domains.

Erkki Koort is also Security pages editor in newspaper *"Postimees"* focusing on security, safety, foreign policy, defence etc., and the author of several books.

Anthony Seaboyer

Anthony Seaboyer teaches Political Science and Political Philosophy at the Royal Military College of Canada (RMC) as well as the Weaponization of Information for Information Operations, Psychological Operations and Adversarial Information Space Exploitation at the Peace Support Training Centre (PSTC). Anthony is also the editor of the Journal of Future Conflict published by Queen's University. His research focuses on national security primarily regarding information warfare, social influence, psychological warfare, persuasion, social media exploitation, and information warfare activities of Russia, China, Iran, North Korea, armed non-state actors as well as effects of the weaponization of information on democracies. His research has been awarded with over 50 research grants. Anthony is also a contracted CBC Network Commentator and Regular Guest Commentator for CTV News Channel on National Security developments. He frequently appears also on other national and international media such as the BBC and Al Jazeera.

Hanno Pevkur

Hanno Pevkur is an Estonian Politican, Member of the Parliament of Estonia and Former Chairman of the Estonian Reform Party. He has served as the Minister of Social Affairs from 2009 to 2012, as the Minister of Justice from 2012 to 2014 and as the Minister of the Interior from 2014 to 2016.

Additional links:

- https://en.wikipedia.org/wiki/Hanno_Pevkur
- https://www.riigikogu.ee/en/parliament-of-estonia/composition/members-riigikogu/saadik/cf42a56a-b91a-4a51-913b-a489305326a2/Hanno-Pevkur

Jonatan Vseviov

Jonatan Vseviov graduated from the University of Tartu with a degree in Political Science and then obtained a master's degree in Security Studies at the Georgetown University. In 2004, Vseviov joined the Policy Planning Department at the Foreign Ministry, and then moved to the Estonian Embassy in Washington as a Policy Diplomat. Between 2008 and 2018, Vseviov worked at the Ministry of Defence, serving as the Undersecretary for Defence Planning from 2014 to 2016, and as the Secretary General from January 2016. From August 2018, Jonatan Vseviov has been the Estonian Ambassador to the United States.

Teemu Tammikko

Dr Teemu Tammikko works as a policy officer focusing on countering hybrid threats in the Security and Defence Policy Directorate of the European External Action Service, and he is an Adjunct Professor of Political Science in the Tampere University, Finland. Previously he has worked as a Visiting Expert in the Ministry for Foreign Affairs of Finland, and as a Researcher in the Finnish Institute of International Affairs, Danish Institute

of International Studies, and University of Tampere. Tammikko has published widely on political violence, terrorism, protest movements, and European security politics. He has also worked as a Team Leader in the EUMM Georgia, and as a political analyst in EUFOR Althea, Bosnia and Herzegovina.

Arnold Sinisalu

Dr Arnold Sinisalu has served as a Director General of the Estonian Internal Security Service (KAPO) since 2013. He has been working at KAPO since 1993, mainly in managerial positions, including the position of Deputy Director General of KAPO. Arnold Sinisalu holds a PhD in Law from the University of Tartu (2012), his doctoral dissertation was titled *"Restrictions to Subversive Leverage in International Law".*

Additional link:

- https://www.etis.ee/CV/Arnold_Sinisalu/eng

Mark Voyger

Mark Voyger is currently a Senior Non-Resident Fellow at the Center for European Policy Analysis (CEPA), Washington, D.C., and Vice President for Strategic Studies and Multi-National Programs with TheTacNet.com online training company. Previously, in 2019-2020, he was a Senior Scholar at the Penn Biden Center for Diplomacy and Global Engagement in Washington, D.C. In 2018-2019 he taught Russian and Eastern European politics and security as the Senior Lecturer at the Baltic Defence College in Tartu, Estonia. Prior to his academic career, in the period 2013-2018, he served as the Special Advisor for Russian and Eurasian Affairs to the Commanding General of US Army Europe in Wiesbaden, Germany, and as the Cultural Advisor and Senior Russia Expert at NATO's Allied Land Command in Izmir, Turkey. In the period 2009-2013 he was deployed to Iraq and Afghanistan as an advisor and social scientist with the US Army. He also worked for Senator Mitt Romney's Presidential campaigns as a member of the Executive Department (2007-2008) and the Russia Advisory Group (2011-2012).

He holds a Master of Arts in Law and Diplomacy degree from the Fletcher School of Law and Diplomacy at Tufts University with a focus on Russia-NATO relations, and a Master of Public Administration degree from Harvard University's Kennedy School of Government, and he has read for a PhD in Middle Eastern Studies at Cambridge University, UK.

Mark Voyger's areas of academic and professional expertise include Eastern European, Balkan and Middle Eastern politics and security issues, Russian foreign and security policy, Russian military strategies and doctrine, hybrid warfare, as well as trans-national Islamist ideologies and movements.

Mr Voyger is fluent in Russian, Ukrainian, Bulgarian, Arabic, Turkish, French, Spanish and Italian. He has written and spoken understanding of German, Portuguese, Serbo-Croatian, and Macedonian, and basic knowledge of Hindi, Farsi, Hebrew and Greek.

DAY 2

Vasyl Bodnar

Vasyl Bodnar started his career in foreign policy of Ukraine in 1998 serving as an Attaché and as a Third Secretary of Balkan Desk in the Ministry of Foreign Affairs of Ukraine. His diplomatic career covers the service as the Secretary in Embassy of Ukraine to the Russian Federation in Moscow during 2000-2004, afterwards as an Acting Head of Turkey and South Caucasus Desk in Kyiv. Mr Bondar served during 2006-2010 as First secretary and Counselor in Embassy of Ukraine to the Republic of Poland, Warsaw, followed by his next assignment as a Deputy Director General of the Third Territorial Department (Eastern and Northern Europe) in the Ministry of Foreign Affairs in Kyiv. During 2013-2017 he served at various diplomatic positions as a Minister Counselor in Embassy of Ukraine to the Republic of Turkey in Ankara; as a Consul General of Ukraine in Istanbul, as Representative of Ukraine to the BSEC Organization and as an Acting Director, Director of the Second European Department in the Ministry of Foreign Affairs of Ukraine.

Since November 2017, Mr Bondar is a Deputy Minister of Foreign Affairs of Ukraine.

Mark Galeotti

Dr Mark Galeotti is an expert in modern Russia, especially its security politics, intelligence services and criminality. He is a Director of the Consultancy Mayak Intelligence, as well as an Honorary Professor at University College London and a Senior Associate Fellow of the Royal United Services Institute. A prolific author, his most recent books include *The Vory: Russia's super mafia* (Yale, 2018), *Russian Political War* (Routledge, 2019), *We Need To Talk About Putin* (Ebury, 2019) and the forthcoming *The Weaponisation of Everything* (Yale, 2022). He also writes regularly for the *Moscow Times, Raam op Rusland, Spectator* and many other outlets. He read history at Robinson College, Cambridge, and took his doctorate in politics at the London School of Economics. He has been Head of History at Keele University, Professor of Global Affairs at New York University, a Visiting Professor at Rutgers-Newark (Newark), Charles University (Prague) and MGIMO (Moscow), and a Senior Research Fellow at the Foreign & Commonwealth Office. He has advised and given evidence to a wide range of bodies, from the UK House of Commons Foreign Affairs Committee and the NATO Parliamentary Assembly to Interpol and SHAPE. He is currently working on a series of projects, including a study of Russia's intelligence services and their impact on Kremlin policy-making and a history of the evolution of organised crime.

Vladimir Sazonov

Dr Dr Vladimir Sazonov works as a Research Fellow at Estonian Academy of Security Sciences, as a Senior Research Fellow at Estonian Military Academy and as an Associate Professor at the Centre for Oriental Studies in the University of Tartu. He teaches lectures on politics, history and security (Middle-East, Russia). His research fields comprise hybrid warfare, Middle-Eastern, Russian state ideology and information war. Sazonov published articles, several books and volumes (e.g. Tartu University Press 2010 and 2017; Jim Eisenbraun (Penn State University Press) 2016; Äripäev 2020; Springer 2021 etc.) on Russian state ideology, propaganda, Middle-Eastern history, politics and security.

Jessikka Aro

Jessikka Aro is an awarded investigative reporter with the Finnish Broadcasting Company. Aro specializes in Russia, extremism and information warfare. In 2014 she started to investigate the pro-Kremlin social media trolls techniques and influence on public debates outside Russia's borders. Due to her investigations, she became the target of a severe and still ongoing international propaganda and hate speech campaign. In 2019 Aro published a best-selling investigative book about Kremlin's information warfare in Finnish, and the book is translated to several languages. She trains reporters and the public to recognize and counter online disinformation. Aro is also lobbying for better legislation to counter hybrid threats and protect citizens from state-sponsored online security threats, and she has witnessed in the US Congress. In 2019 the US State Department awarded her with the International Women of Courage Award, but the award was mysteriously rescinded by president Donald Trump's administration due to her social media criticism of President Trump.

Holger Mölder

Dr Holger Mölder is Estonian political scientist, Associated Professor in International Relations and Security Studies at the Tallinn University of Technology (TalTech). He has PhD in Political Sciences from the University of Tartu and MA in International Security and Civil Military Relations from the US Naval Postgraduate School. Previously, he worked nearly 20 years for the Estonian Ministry of Defense and the Estonian Military Academy. His main research interests cover various international security issues, political cultures, influence and information operations, and psychological warfare. His most recent publications are *Culture of Fear: The Decline of Europe in Russian political imagination* (in Krouwel, A.; Önnerfors, A. (Ed.). *Continent of Conspiracies: Conspiracy Theories in and about Europe* (Abingdon-on-Thames, England, UK: Routledge) and a book *The Russian Federation in the Global Knowledge Warfare - Influence Operations in Europe and Its Neighborhood.* (Springer Nature) (edited with A. Chochia, T. Kerikmäe and V. Sazonov).

Andreas Ventsel

Dr Andreas Ventsel is an Associate Professor of Semiotics at Tartu University and a lecturer in Pallas University of Applied Sciences in Tartu. His research is interdisciplinary which includes semiotics, discourse theory, visual communication, rhetoric and political analysis. He has presented the results of the research on these topics in around 100 academic articles and been the initiator and editor of several international scientific journals. Ventsel is the author the books *Strategic Conspiracy Narratives: A Semiotic Approach* (Routledge, 2020), co-author M.-L. Madisson, and *Introducing Relational Political Analysis - Political Semiotics as a Theory and Method* (Palgrave Macmillan, 2020), with P. Selg.

Mari-Liis Madisson

Dr Mari-Liis Madisson is a Researcher of Semiotics at Tartu University. Her research interests lie primarily in cultural semiotics, media semiotics and political semiotics. Since 2014 she has taught multiple courses on online culture and critical media literacy. She is the author of *The Semiotic Construction of Identities in Hypermedia Environments:*

The Analysis of Online Communication of the Estonian Extreme Right (Tartu University Press, 2016) and *Strategic Conspiracy Narratives: A Semiotic Approach* (Routledge, 2020), co-author A. Ventsel.

Alina Frolova

Alina Frolova, CDS Deputy Chairman, is a strategic communications expert and civic activist, co-founder of CDS, founder and advisor to Stratcom Ukraine NGO established to support governmental communications development in Ukraine and CORE Reputation Management Agency. Alina has more than 20 years of experience in strategic communications, brand development and advocacy, loyalty and consumer behavior management for multinational and Ukrainian leading companies, in addition leading 50+ communication projects for governmental and public agencies, among them MOH, MFA, MOD, MOE and others. She is the Initiator of Invictus Games Team Ukraine project and Leading Expert in governmental communications, Project lead for Ukraine-NATO Strategic Communications Partnership Roadmap implementation (2015-2019). Alina is a co-founder of Ukraine Crisis Media Center (2014), she was from 2015 until 2016 an advisor to Deputy Minister MOD UA, from 2015 until 2019 an advisor to Minister of Informational Policy of Ukraine on strategic communications, in charge of governmental StratCom capacity building, cooperation with NATO and other security and defence partners, in 2019 joined Ministry of Defence as a Deputy Minister responsible for defence cooperation. While being a Deputy Minister paid special attention to the BASR security aspects and UKR Navy development. She has a master's degree in Political Science and International Relations (Kyiv State University), diploma in Public Relations of the Chartered Institute of Public Relations (London).

José Casimiro Ferreira Morgado

José Casimiro Ferreira Morgado practiced as a lawyer, until 1997. From 1991 to 2008 he was a professor at the Faculty of Law of the Lusíada University of Porto. In November 1997, he was appointed as a Regional Director of the Security Intelligence Service (SIS) in Porto. In April 2008 he became the Chief of Staff of the Secretary-General of the Intelligence System of the Portuguese Republic. His professional career covers working as the Director-General of the Strategic Defense Intelligence Service (SIED) during 2010 until 2019.

José Casimiro Ferreira Morgado started as the Director EU Intelligence and Situation Centre (INTCEN) in September 2019.

REFERENCES

Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions on the EU Security Union Strategy Brussels, 24.7.2020 [www] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0605 (last visit 7.10.2021)

Countering hybrid threats: Council calls for enhanced common action. The Council of the EU, 10.12.2019 [www] https://www.consilium.europa.eu/en/press/press-releases/2019/12/10/countering-hybrid-threats-council-calls-for-enhanced-common-action/ (last visit 20.10.2021)

EU Commission president accuses Belarus of launching 'hybrid attack' against Europe, 15.09.2021 [www] https://www.aa.com.tr/en/europe/eu-commission-president-accuses-belarus-of-launching-hybrid-attack-against-europe/2365349 (last visit 7.10.2021)

Giles, K., Seaboyer, A. 2020. Russia in the Grey Zone. Defence Research and Development Canada

INTERNAL SECURITY INSTITUTE OF THE ESTONIAN ACADEMY OF SECURITY SCIENCES, IN A CLOSE COOPERATION WITH THE INTELLIGENCE COLLEGE IN EUROPE, HELD A WEB-BASED SEMINAR ON HYBRID THREATS AND THEIR IMPACT ON EUROPEAN SECURITY IN TALLINN, ESTONIA, ON 16–17 JUNE 2021.

At the event, many distinguished speakers from Estonia, Ukraine, Finland, UK, US, Canada, and EU were represented, covering different angles of hybrid threats and their methods. The target group of the event were leaders and senior officials of European security and intelligence services, law enforcement authorities, representatives of respective ministries, and educational institutions. The seminar gave the audience an overview of hybrid threats from the perspective of politicians, policy makers, researchers, and practitioners.

sisekaitse.ee