REPORT

Resilience Against Disinformation

A New Baltic Way to Follow?

| Dmitri Teperik | Solvita Denisa-Liepniece | Dalia Bankauskaitė |
| Kaarel Kullamaa |

OCTOBER 2022

RKK ICDS
RAHVUSVAHELINE KAITSEUURINGUTE KESKUS
INTERNATIONAL CENTRE FOR DEFENCE AND SECURITY
EESTI · ESTONIA

Title: Resilience Against Disinformation: A New Baltic Way to Follow?

Authors: Teperik, Dmitri; Denisa-Liepniece, Solvita; Bankauskaitė, Dalia; Kullamaa, Kaarel

Publication date: October 2022

Category: report

Cover page photo: Runners take part in a traditional relay race Vilnius-Riga-Tallinn dedicated to the 30th anniversary of the Baltic Way on 23 August 2019 (photo by Mindaugas Kulbis / Associated Press / Scanpix)

Keywords: disinformation, malignant influence, media, media literacy, resilience, security, society, vulnerability, Baltic states, Estonia, Latvia, Lithuania, Russia, China

Disclaimer: The views and opinions contained in this paper are solely those of its authors and do not necessarily represent the official policy or position of the International Centre for Defence and Security, or any other organisation.

ISSN 2228-0529

ISBN 978-9916-709-02-3 (print)
978-9916-709-03-0 (pdf)

63/4 Narva Road
10120 Tallinn, Estonia
info@icds.ee, www.icds.ee

Table of Contents

ACKNOWLEDGEMENTS

To become a successful journey, every analytical study requires productive teamwork, as well as efficient synchronisation of research, management and communication efforts. This report is only a visible part of the 2-year-long project, inspired and executed by pan-Baltic cooperation between four authors. Our entire team is grateful for the valuable contributions and enriching insights that over 60 respondents from Estonia, Latvia and Lithuania have provided during in-depth interviews. Furthermore, we appreciate the great help from ICDS interns Lorenzo Crippa, Christina Hill and Isabella Martin for their useful remarks and suggestions on the report. We also thank Tomas Jermalavičius, whose advice helped to structure this report, and Tetiana Fedosiuk for her diligent editorial work.

Part of this research was supported by the Open Information Partnership (OIP).

About the Authors

Dmitri Teperik

Dmitri Teperik has been the Chief Executive and the Member of the Management Board at ICDS since 2016. He is a director of several ICDS development and cooperation projects in Ukraine, as well as of the outreach activities in the Baltic states. In 2007-15, he worked at the Estonian Ministry of Defence, overseeing research and development (R&D), as well as the defence industry. In 2016, he co-founded "Resilience League", an international training and co-operation platform, to provide young professionals and experts with practical skills and tools necessary to develop cognitive resilience against hostile disinformation and societal polarisation. Since 2016, he has been leading "Resilient Ukraine", a development and cooperation programme that focuses on measuring and strengthening national resilience in vulnerable communities in Ukraine. Among his main academic interests are factors contributing to national resilience, situational awareness in the information environment and social media, as well as interdependencies between communication and behaviour. He holds an MS degree from the University of Tartu (Estonia) and has completed various internships abroad, including at Vilnius University (Lithuania) and NATO HQ. He has participated in various professional training courses on security in Estonia, Latvia, Lithuania, Georgia, Belgium, Germany, France, Spain, the Netherlands, the USA, Canada, as well as NATO and the EU.

Solvita Denisa-Liepniece

Dr. Solvita Denisa-Liepniece is a disinformation resilience advisor at the Baltic Centre for Media Excellence (BCME) and an Assistant Professor at Vidzeme University of Applied Sciences (Latvia). In 2021-22, she was a Visiting Scholar at the Jordan Centre for Advanced Study of Russia, New York University. Previously, she was an Associate Research Scholar at Yale University (Juris Pageds Visiting Fellow, 2020). She also served as a country expert for several international organisations focusing on information resilience in the Baltic states. She completed her Ph.D. at the University of Antwerp (Belgium), having written her thesis on political communication in post-Soviet Belarus. Her research interests encompass strategic political communication, intercultural communication and information resilience. In addition to her academic activities, she has built a career in journalism and worked for the Public Broadcasting of Latvia.

Dalia Bankauskaitė

Dalia Bankauskaitė is an interdisciplinary expert in security policy, strategic communication and political consulting. She currently serves as a Non-Resident Senior Fellow at the Center for European Policy Analysis (CEPA), working on the think-tank's Democratic Resilience Program. She teaches strategic communications as a Partnership Associate Professor at Vilnius University and provides expertise to the Swedish Defence University. With decades of experience across government, academia, and consulting, she focuses on advancing the understanding of the total defence doctrine and a whole-of-society approach to security. Her work includes analysis of hybrid aggression and influence operations, as well as building comprehensive media literacy, societal resilience and capacity-building programmes. She has extensive professional experience in strategic communication in Lithuania, Ukraine, Georgia, Bosnia and Herzegovina and the Baltic Sea region. Her career highlights include heading Lithuania's EU Public Information Unit before the country's accession to the EU; acting as the information officer at the European Commission's delegation; and serving at the Lithuanian Embassy in Moscow. She holds an MSc degree from the London School of Economics and Political Science (LSE).

Kaarel Kullamaa

Kaarel Kullamaa worked for the Estonian Foreign Policy Institute at the ICDS during 2021-22. His research centred on Eastern Europe, with a special focus on Russia and EU-Russia relations. His previous studies also addressed strategic communication and addressed the use of digital solutions that enhance state-building and security. He worked as an intern at the Estonian Foreign Policy Institute at the ICDS and as a project leader and advisor to the City Council of Tartu. Currently, he is a sales manager at Threod Systems, a defence industry company that is a leading manufacturer of multiple UAV platforms and supplementary sub-systems in Estonia. He has a BA degree in Government and Politics from the University of Tartu (Estonia) and St. Petersburg State University (Russia) and holds a MA degree in European Studies from Aarhus University (Denmark). Additionally, he completed further training on cyberspace and the state, organised by Oxford University's Cyber Studies Programme and the University of Tartu's Centre for the Information Society.

List of Acronyms

AI	Artificial Intelligence
BRELL	Belarus-Russia-Estonia-Latvia-Lithuania
CCP	Chinese Communist Party
CESA	Continental Europe Synchronous Area
CERT.LV	Computer Emergency Response Team Latvia
CIS	Center for Internet Security
CoE	Centre of Excellence
COVID-19	Coronavirus Disease of 2019.
CSO	Civil Society Organisation
DDoS	Distributed Denial-of-Service
DRI	Disinformation Resilience Index
ETV	*Eesti Televisioon* [Estonian Television]
ERR	*Eesti Rahvusringhääling* [Estonian Public Broadcasting]
EU	European Union
FSRU	Floating Storage and Regasification Unit
GIPL	Gas Interconnection Poland–Lithuania
GONGO	Government-Organised Non-Governmental Organisation
ID	Identity Document
IPS/UPS	Integrated Power System/Unified Power System
IT	Internet Technology
LNG	Liquefied Natural Gas
MIL	Media and Information Literacy
MPM	Media Pluralism Monitor
NATO	North Atlantic Treaty Organisation
NCSI	National Cyber Security Index
NGO	Non-Governmental Organisation
NPP	Nuclear Power Plant
OK	*Odnoklassniki*
PBK	*Pervyj Baltijskij Kanal* [First Baltic Channel]
PKN Orlen	*Polski Koncern Naftowy Orlen* [Polish Oil Concern Orlen]
RIA	*Riigi Infosüsteemi Amet* [Information System Authority]
ROC	Russian Orthodox Church
SAB	*Satversmes aizsardzības birojs* [Constitution Protection Bureau]
StratCom	Strategic Communications
UK	United Kingdom
USA	United States of America
USSR	Union of Soviet Socialist Republics
WWII	World War II, Second World War
VDD	*Valsts drošības dienests* [Latvian State Security Service]
VK	VKontakte
VSD	*Valstybės saugumo departamentas* [State Security Department]

Executive Summary

The Baltic states, although not immune to disinformation, possess unique experience and knowledge pertaining to effective methods to resist and combat this malice. This report is based on in-depth semi-structured interviews and supplementary surveys conducted with the representatives of several clusters – media, civil society organizations, state institutions, think-tanks/academia and business communities. It aims to assess risks and vulnerabilities, as well as the three nations' preparedness to counteract foreign-led disinformation. This report also reviews the existing indices that lead to a greater understanding of the intricate nature and interdependences of resilience-shaping factors at various levels, while contributing the unique Baltic perspective to the evolving, global study of disinformation.

Foreign-led disinformation usually targets specific vulnerable communities using a broad range of instruments and strategies, accompanies malicious influence activities and constructs harmful narratives in certain strategically important areas or sectors. Measures to counter these attacks have been the forefront initiatives for the Baltic countries since the restoration of their independence. The report identifies the known vulnerabilities and long-term responses within energy, technology, socio-economic, socio-political, strategic communications and media domains. The start of a major inter-state conventional war in Europe – Russia's full-scale invasion of Ukraine – in February 2022 has triggered a multitude of changes in the information environment of the Baltic states and prompted some radical adjustments and responses. Although these changes are not covered by the report, it is important to consider that neither the exploitation of vulnerabilities in the Baltics by Russia during this war nor the responses of the Baltic governments come in a vacuum. The report thus provides useful background and context that will help to understand what conceptual, legal, policy, institutional, political and societal precursors shape the current situation and determine successes or failures of Russia's and China's disinformation and Baltic counter-disinformation efforts.

Several overlapping crises of 2020-21 – ripple effects from the political upheaval in Belarus, surge in illegal migration engineered by the regime in Minsk, the COVID-19 pandemic and accompanying socio-political perturbations, as well as China's economic and diplomatic coercion against Lithuania – served as a reminder that the Baltic states could not afford standing still in their efforts to strengthen national resilience. While not fundamentally altering the overall landscape of threats and vulnerabilities, these crises were amplified and exploited by malignant disinformation campaigns and foreign interference, therefore changing the security context, testing national resilience and requiring reassessments of the institutional or policy responses in all three countries.

Following a thorough assessment of cyber vulnerabilities, **Lithuania** simultaneously pursues two parallel directions in addressing this challenge: building up national capabilities and strengthening multinational capacities via EU cooperation and mutual assistance mechanisms. Although the country has become one of the international leaders in cybersecurity, the greatest threat to its information and cybersecurity comes from Russian and Chinese intelligence services. The need for the whole-of-society approach to security and defence in general – and to digital security in particular – is well acknowledged and institutionalised, while growing awareness among state institutions, businesses and the public gives grounds for cautious optimism. High-quality multi-lingual media and a coordinated approach to media and information literacy are essential and should be reinforced by comprehensive integration and inclusion programmes for the most vulnerable populations, such as socio-economically deprived groups, ethnolinguistic minorities and new immigrants. Lithuania proved to be more resilient to the pandemic-related disinformation and anti-Western narratives that threatened to increase societal fragmentation and polarisation, having started to build an agile and proactive institutional and educational framework well before 2020-21. The debate about the importance of civil, non-violent resistance in national defence has been high on the political agenda. This debate builds upon the civil society's ongoing contribution to resilience, whose multiple stakeholders are directly engaged in information monitoring, fact-checking and strengthening society's media and information literacy, with combined efforts by volunteers from the IT, media, academia, education and business sectors. Some of these models and approaches are already applied internationally.

Latvia has increased capabilities for mobilisation towards a whole-society approach to cyber and information security, bearing in mind weaponisation of big data ecosystems, hard-to-analyse audio and visual content, problematic user behaviours and evolving media consumption, as well as technological dependence on China. Russia's weaponisation of history and use of entertainment to spread disinformation has been flagged as a new risk vector. Traditional pro-Kremlin agents of influence reduced their visibility and political activities indicating changes of tactics by Russia: strengthening anti-institutional voices based on political and ideological parallelism, urban-countryside gap and openness to populism. At the same time, China has noticeably increased its operations. Wary of the risks of amplification of disinformation, inappropriate fact-checking and trivialisation of the cognitive processes, the main challenge of an institutional response now lies in the necessity to act according to liberal democratic values, with civil society joining forces with the government.

Having ensured that state systems are built to European or US hardware and cryptographic standards, **Estonia** has been able to turn the disruptive attempts into an opportunity by becoming a leading promoter of digitalisation and cybersecurity. China's influence is expanded through corporate takeovers, dependence on Chinese mass production and vulnerability to digital warfare, countering which requires a long-term China strategy. With the popularity of foreign social media platforms and limited options to regulate their content, dissemination of disinformation has become more strategic, designed to gain influence over a longer period while avoiding direct confrontation or conflict. Amid the ethnic gap in society slowly narrowing, an increase in polarisation and radicalisation, especially via the so-called alternative media, is noted along the conservative and liberal axis. The new challenges – such as poor choice of primary sources, reckless transposition of narratives and insufficient fact-checking – warrant systematic analysis of the public information space based on big data and AI-enabled tools that would identify, detect and pre-emptively stop the spread of disinformation.

Follow-up surveys in the wake of those crises, conducted in late 2021, revealed that **Lithuanian** respondents assessed societal preparedness for rapid mobilisation during the multifaceted crisis as 'intermediary', and **Latvian** respondents rated counter-disinformation and resilience-related measures as 'rather poor.' **Estonian** respondents, however, reported positive changes in the level of institutional development and comprehensiveness of the legal framework. Across all three countries, government officials tend to have a more positive view on the ability to protect vulnerable groups, whereas academics/think-tankers highlight a noticeably lower number of strengths and opportunities. The business cluster stressed the need to improve public/private partnerships in order to identify and handle threats, with the state assuming the leading role. Low societal preparedness to mitigate multi-layered information crises that require more coordination and cooperation between various stakeholders is one of the major challenges to Baltic states.

As an important background for resilience, the general strength of the Baltic states arises from historical memory and unique regional context. Western-focused internationalisation in all spheres has proven beneficial to combatting foreign-led disinformation, which strengthens electoral integrity and ensures continued democratic traditions. With result-oriented training courses on cognitive security gradually embedded in formal and informal education, efforts should be redoubled as education remains a key enabler for resilience. The topic of migration should be closely monitored not only by respective authorities but also by media and civil society organisations. National resilience to disinformation can be maintained and further increased by investing in national and local high-quality media. Resilience – as a whole-of government and whole-of society effort – requires all stakeholders, as well as the media, to cooperate. A team-of-teams model should be considered as a feasible practical concept for supporting multi-layered cross-sectoral networking.

Introduction

The Baltic states of Estonia, Latvia and Lithuania are often referred to as states that possess valuable experience in and have practical knowledge of effective methods for resisting Kremlin-led or inspired disinformation and minimising its consequences for the targeted groups and affected societies in general. There is a consensus about sufficient evidence on information activities that have been orchestrated by or from Russia for decades.[1] Despite relative success in this area, the Baltic societies are, nevertheless, still vulnerable to disinformation: in 2021, just 25% of Estonians, 19% of Latvians and 11% of Lithuanians verified online information found on websites or social media.[2] The COVID-19 pandemic highlighted the cognitive vulnerability of certain societal groups to manipulation and conspiracy theories.[3] Moreover, the Baltic societies are not immune to dangerous side effects – such as the spread of disinformation or widening fragmentation and polarisation in societies – of rapidly developing online social networks, digital media and virtual reality technologies.[4]

> *The Baltic societies are not immune to dangerous side effects of rapidly developing online social networks, digital media and virtual reality technologies*

This report is aimed at conducting a common analytical assessment of national vulnerabilities and risks, as well as preparedness to counteract foreign-led disinformation in Estonia, Latvia and Lithuania. This report will also articulate policy recommendations regarding structural actions to strengthen their resilience to disinformation in a long-term. Conducted in 2020-21, this qualitative study focuses on an interdisciplinary evaluation of societies' exposure to the foreign-led disinformation and the level of national resilience to campaigns of hostile influence orchestrated from abroad.

This report is based on the summary of the in-depth semi-structured interviews and supplementary surveys conducted with the representatives of media, civil society organisations (CSOs), state institutions (including defence, security and intelligence authorities), academia and think-tanks, as well as business communities in Estonia, Latvia and Lithuania (henceforth referred to as 'clusters').[5] The first round of the interviews was conducted in summer and autumn 2020, and then the following survey of perceptions was repeated with the same interviewees one year after, in late summer / early autumn 2021, in order to re-assess the situation from the view of recent developments (e.g. crisis in Belarus, domestic politics in the Baltics and, of course, the COVID-19 pandemic). Twenty representatives from five clusters in each Baltic country shared their insights and perceptions during 60 in-depth interviews, the structure of which was based on 33 substantial questions regarding population exposure to foreign-led hostile influence and disinformation campaigns, assessment on preparedness and quality of systemic responses in country, and threats in virtual environment

[1] *GEC Special Report: Pillars of Russia's Disinformation and Propaganda Ecosystem* (Washington D. C.: U.S. Department of State, August 2020); Todd C. Helmus et al., *Russian Social Media Influence: Understanding Russian Propaganda in Eastern Europe* (Santa Monica, CA: Rand Corporation, 2018); Vera Michlin-Shapir, David Siman-Tov, and Nufar Shaashua, "Russia as an Information Superpower," in *Cognitive Campaign: Strategic Intelligence Perspectives*, eds. Yossi Kuperwasser and David Siman-Tov (Tel Aviv: Institute for National Security Studies, 2019), 115–132.

[2] "How many people verified online information in 2021?" *Eurostat*, 16 December 2021.

[3] Re:Baltica, "Who spreads vaccine lies in the Baltics?" *LRT*, 2 March 2021; "Debunk EU: Latvia had the widest spread of COVID-19 related disinformation in May," *Delfi*, 11 June 2020.

[4] Anne Applebaum and Peter Pomerantsev, "How to put out democracy's dumpster fire," *The Atlantic*, 11 March 2021.

[5] If grouped, then referred as "sectors" or "clusters" in further sections of the report: 1. media experts and journalists; 2. representatives of state authorities related to strategic communication, public relations, counterintelligence, internal security or defence; 3. scholars and experts from academia and think-tank community; 4. civil society organisations and individual civic activists; 5. representatives of business community and opinion leaders in private sector. As a general remark, it should be noted that experts from academia and civic society cluster were more approachable for in-depth interviews than the representatives of other clusters.

and digital vulnerability of society.[6] Additionally, the interviewed respondents were asked to complete a short survey questionnaire based on a Likert-type scale to assess sectoral perspective and developments in 2020 and 2021. The consolidated picture gives a broad overview of their perception of resilience to malignant influence and disinformation in the Baltics.

Chapter 1 outlines several difficulties in making comprehensive and reliable cross-country assessments of national resilience and reviews some of the previous efforts made, particularly in relation to the Baltic states. The report then describes the state of play and its perception by the respondents as of 2020-21. Chapter 2 highlights similar and different characteristics of the Baltic states in terms of well-known vulnerabilities that have been identified for a long time. Chapter 3 outlines new perceived challenges and emerging risks, and pays special attention to the implications of various overlapping security crises, including the COVID-19 pandemic, that afflicted the region during those two years for information security and media landscape in the Baltics. Chapter 4 identifies key differences between the groups of respondents in their assessments of main vulnerabilities and measures undertaken to mitigate those vulnerabilities. The report ends with the conclusions and policy recommendations for improving the situational awareness and co-operation between the states – regionally and between various national sectors. Moreover, the report provides suggestions on how resilience to disinformation could be assessed in the Baltics through developing and validating variables for a score-based index in the future.

Given the Russian full-scale military attack against Ukraine, which has led to rapid developments in European security since late February 2022, the authors acknowledge the retrospective look of the report as well as the absence of focus on the immediate and long-term consequences of Russia's war against Ukraine as it relates to information resilience of the Baltic states.[7] During the time of the report's preparation for the release, however, some useful data points began emerging. For instance, as of spring 2022, 74% of Estonians, 72% of Latvians and 62% of Lithuanians supported the total ban of the webpages and actors spreading disinformation about the war in Ukraine.[8] These and other related topics should be addressed by the academic community and policy experts in future efforts to assess resilience of the Baltic states. This report, on the other hand, offers a useful snapshot of two pre-war years that could serve as a basis for assessing the extent of change and continuity since the start of the war.

1. Challenges for Comparative Research on Resilience

Arguably, some parts of the accumulated Baltic experience can be extrapolated onto other countries that are facing similar challenges in counteracting foreign-led disinformation, which is a well-researched and documented assertion.[9] Yet, given the historical context and combination of various cultural, economic and socio-political factors, the Baltic 'know-how' has several unique features – either in general as a whole region, or in terms of specific national idiosyncrasies. It provides not just

[6] In this report, disinformation as phenomenon was analysed as defined in the following study: Maria D. Molina et al., "“Fake News” Is Not Simply False Information: A Concept Explication and Taxonomy of Online Content," *American Behavioral Scientist* 65, no. 2 (February 2021): 180–212. By foreign-led disinformation campaign, the malign influence of Russia and China is considered by the authors to be most relevant in the context of the Baltic states, where Chinese disinformation activities are relatively new phenomenon while those of Russia have been experienced, studied, analysed and countered over several decades. Given the multidimensional notion of resilience, the report's authors attempted to gasp and reflect it in this study from several viewpoints. As malicious disinformation campaigns can be built upon variety of combinations from different sectors, the authors of the report adopted and analysed an expanded view of inter-related vulnerabilities, including some aspects of espionage, economic influence activities, historical memories, patterns of media consumption, status of democracy, energy and cyber security, ethnic minorities etc.

[7] Foremost, it applies to the national and international sanctions against Russia which have effect on energy market of and media landscape in the Baltics. Moreover, emerging implications shape also alienating perceptions among majority in the Baltics against everything which is or might be related to Russia, including relations in the spheres of business, culture, education etc.

[8] Dominika Hajdu et al., *GLOBSEC Trends 2022: CEE amid the War in Ukraine* (Bratislava: Democracy and Resilience Centre at GLOBSEC, 2022); "Baltics, Poland turn to social media networks over Russian disinformation," *The Baltic Times*, 28 February 2022.

[9] Lukas Andriukaitis, *Russian Propaganda Efforts in The Baltics and the Wider Region* (Vilnius: Vilnius Institute for Policy Analysis, 2020).

some research substance to satisfy academic curiosity in general, but also reflects on some challenges for specialists and practitioners in conducting a validated cross-national comparison either internally within the Baltics or externally between the Baltic states and other countries.[10] An accurately weighted scale is needed for an adequate comparison of the three countries.

Hostile influence campaigns that include persistent disinformation fall into the category of chronic stressors

Inspired by successful quantitative assessments (e.g. Global Cyber Security Index, National Cyber Security Index, FM Global Resilience Index), the aspiration to standardise a measurement of resilience in practice has always faced complex challenges and obstacles – starting from the validation of relevant indicators and finishing with data accuracy and synchronisation of measurement efforts.[11] Various scoreboards quantify and visualise some specific parameters of resilience in societal development, emergency preparedness or, multidimensionally, at a community level.[12] As risk and probability scholar Nassim Taleb argues, "there are many definitions of resilience, the best of which include proactive pre-crisis preparations and risk mitigation, effective incident management and leveraging whatever shocks occur to build back better."[13] This, however, places emphasis on measuring preparedness for and in response to sudden shocks, or 'acute' stressors, but is less useful in understanding the impact of 'chronic' stressors that influence societies over the extended periods of time and in assessing the effectiveness of coping mechanisms when dealing with such stressors.[14]

Hostile influence campaigns that include persistent disinformation fall into the category of *chronic stressors*. Scholars identify several groups of factors within political, media, economic and societal environments that should be considered while assessing the state of resilience to disinformation.[15] In some cases, researchers managed to identify and validate variables that correlate significantly with susceptibility to disinformation.[16] Conceptual frameworks for researching disinformation can also serve as a strong starting point to structure a comparison study on the state of information resilience.[17] Various case studies across the member states of the European Union (EU) provide insights and best practices on how to conduct strategic communications to counter hybrid threats and their components.[18] Conducted on a larger international scale, policy studies can also provide recommendations on legislative and policy measures for mitigating undesirable effects of disinformation.[19] Moreover, the combination of different numeric indices (e.g. populism index, polarisation index, media trust index, social media index, social progress index, etc.) can provide quantitative inputs for a generalised picture, although with limitations related to national or regional specificity.

[10] Ilaria La Torre, *The Baltic's response to Russia's Threat – How Estonia, Latvia and Lithuania reacted to the recent actions of the Russian federation* (Brussels: European Army Interoperability Centre, 2020).

[11] International Telecommunication Union, "Global Cybersecurity Index," last accessed 18 August 2022; e-Governance Academy, "National Cyber Security Index. Methodology," last accessed 18 August 2022; FM Global, "2022 FM Global Resilience Index," last accessed 18 August 2022.

[12] Centre for Sustainable Peace and Democratic Development and UNDP-ACT, "SCORE Ukraine. Methodology," last accessed 18 August 2022; Christopher G. Burton et al., *Resilience Performance Scorecard (RPS) Methodology. Version 1.6* (GEM Foundation, September 2017); Lesley Edgemon et al., *Community Resilience Indicator Analysis: County-Level Analysis of Commonly Used Indicators from Peer-Reviewed Research, 2020 Update* (Argonne National Laboratory, Federal Emergency Management Agency, 2020).

[13] Nassim Nickolas Taleb, *Antifragile: Things That Gain From Disorder* (New York: Random House, 2012).

[14] On different nature of stressors and corresponding coping mechanisms see, for instance: Seymour Spilerman and Guy Stecklov, "Societal Responses to Terrorist Attacks," *The Annual Review of Sociology* 35, no. 1 (August 2009): 167–189.

[15] Edda Humprecht, Frank Esser, and Peter Van Aelst, "Resilience to Online Disinformation: A Framework for Cross-National Comparative Research," *The International Journal of Press/Politics* 25, no. 3 (July 2020): 493–516.

[16] Michael X. Jin et al., "Novel Validated Index for the Measurement of Disinformation Susceptibility at the County Level," *Cureus* 13, no. 5: e15305.

[17] Claire Wardle and Hossein Derakhshan, *Information Disorder. Toward an interdisciplinary framework for research and policymaking* (Strasbourg: Council of Europe, October 2017).

[18] Juan Pablo Villar García et al., *Strategic communications as a key factor in countering hybrid threats* (Brussels: European Parliament, March 2021).

[19] Judit Bayer et al., *Disinformation and propaganda: impact on the functioning of the rule of law and democratic processes in the EU and its Member States. 2021 update* (Brussels: European Parliament, April 2021); Jon Hassain, *Disinformation in Democracies: Improving Societal Resilience to Disinformation* (Riga: NATO Strategic Communications Centre of Excellence, March 2022).

Media literacy is just one piece of a puzzle and should not be overestimated or viewed in isolation

As a side effect, international indices that focus on a particular dimension to the exclusion of others might lead to 'beauty contests' between the nations – a rather long-standing characteristic in the relations between the Baltic states – that add little to objective and comprehensive situational awareness. This was the case, for instance, with the Media Literacy Index – according to which Estonia ranked 3rd among the EU nations in 2021, while Latvia and Lithuania ranked 20th and 18th respectively – which inevitably creates the impression that Estonia excels at overall resilience to disinformation.[20] Even though it is recognised as one of the tools against disinformation, media literacy is, however, just one piece of a puzzle and should not be overestimated or viewed in isolation from other aspects.[21]

Another example of a narrowly focused comparison – between the countries of Central and Eastern Europe, including the Baltic states – can be found in the GLOBSEC Trends publications. According to which, for example, 56% of Lithuanians, 48% of Latvians and 31% of Estonians distrusted mainstream media in their countries in 2021.[22] Although it correlates with another source which found that, as of autumn 2021, the trust in public media was almost twice higher in Estonia than in Lithuania or Latvia, it does not provide a full picture of national resilience to disinformation – just one important aspect of it.[23]

The Media Pluralism Monitor (MPM) is a holistic tool designed to identify some potential risks to media pluralism in EU member states and some neighbouring countries. It is yet another sector-specific multi-indicator that provides some insights into the state of resilience to disinformation in various countries, including the Baltic states. According to the MPM, the media landscape is measured annually against various contributing factors that give more of a dynamic perspective on the state of play in this sector, including protection against mis- and disinformation and hate speech. As of 2021, the risks to media pluralism that the Baltic states face were assessed mostly in the low and medium categories, with some exceptions.[24]

73% of Latvians, 78% of Estonians and 86% of Lithuanians consider a foreign power using social media and online tools for disrupting electoral campaigns a serious threat to democracy

There are also indices that add to the understanding of the impact of other factors – including disinformation – on public perception of main challenges to security. A global survey on democracy in 55 countries, for instance, provides comparative insights about sociologically weighted perceptions of citizens on geopolitical issues, global powers, emerging threats and other challenges. Since disinformation and propaganda often play on fears and discords within a society, this survey is instrumental in comparing opinions on challenges and implemented responses by democratic countries not just regionally, but also globally. For instance, 73% of Latvians, 78% of Estonians and 86% of Lithuanians consider a foreign power using social media and online tools for disrupting electoral campaigns a serious threat to democracy.[25]

These many indices might appear overwhelming and unhelpful in ascertaining

[20] Marin Lessenski, "Media Literacy Index 2021," Open Society Institute – Sofia, 14 March 2021.

[21] Cynthia Garcia, *The Baltic Centre for Media Excellence. A Case Study on Media Literacy as a Tool Against Russian Disinformation* (Medford, MA: Tufts University, May 2018).

[22] Dominika Hajdu et al., *GLOBSEC Trends 2021: Central & Eastern Europe one year into the pandemic* (Bratislava: Democracy and Resilience Centre at GLOBSEC, June 2021).

[23] Andres Jõesaar, Anda Rožukalne, and Deimantas Jastramskis, "The role of media in the Baltics. To trust or not to trust?" Baltic Centre for Media Excellence, last accessed 18 August 2022.

[24] Konrad Bleyer-Simon et al., *Monitoring media pluralism in the digital era: application of the Media Pluralism Monitor in the European Union, Albania, Montenegro, the Republic of North Macedonia, Serbia and Turkey in the year 2021* (San Domenico di Fiesole: European University Institute, 2022).

[25] Dominoque Reynié (ed.), *Freedoms at risk: the challenge of the century. A global survey on democracy in 55 countries* (Fondation pour l'innovation politique, January 2022).

Decision-makers need a more substantial understanding of and practical approach to strengthening resilience against hostile and malicious information

the state of resilience in individual societies. Nevertheless, each attempt to make comparisons between different countries or policy domains creates a potentially greater understanding of the multi-layered nature and cross-sectoral interdependencies of resilience-shaping factors at various levels. Looking at different existing indices through the prism of resilience contributes to bringing and linking together academic researchers, a community of practitioners, policymakers and other relevant stakeholders, who should benefit from in-depth analysis and professional evaluation of resilience to disinformation in a dynamic perspective. Since, for instance, media literacy has become an integral part of the political agenda, decision-makers and political actors adopted a rather superficial rhetoric on the issue and therefore need a more substantial understanding of and practical approach to strengthening resilience against hostile and malicious information.[26] To achieve this, they should make better use of applied social sciences to understand and mitigate the effects of disinformation in the targeted populations.[27] Disinformation threats can also be measured and described through a risk-impact approach that weighs the potential impact of various identified risks to information security.[28] Given cross-sectoral challenges within the security environment, decision-makers and government authorities should look for various methods to resolve cognitive-emotional conflicts that arise from disinformation campaigns.[29]

Disinformation-themed research is getting more attention globally and is a well-established research field in the Baltic states.[30] Comprehensive literature databases prove that the state of disinformation has been continuously and profoundly researched separately in each Baltic nation during the last three decades. In addition, many studies have also addressed some specific aspects of disinformation by comparing the three countries to each other or even in the larger groups of Nordic or Central and Eastern European countries. Among others, the NATO Strategic Communications Centre of Excellence, the European Centre of Excellence for Countering Hybrid Threats and the Baltic Centre for Media Excellence make a valuable contribution to joint research efforts in harmonising disinformation-related studies and applicability of their outcomes in the Baltic region.[31] Media Literacy Sector Mapping and regularly conducted Baltic Media Health Check studies are important instruments for analysing various trends and issues of importance in the Baltic media.[32]

Already in 2018, national chapters on Estonia, Latvia and Lithuania within the report on the Disinformation Resilience Index (DRI) in Central and Eastern Europe provided relatively comparable analyses of the respective countries.[33] The report identified differences and similarities between the Baltic countries that are reflected in a variety of approaches implemented by their governments to counter disinformation.[34] In other studies, those comparisons have also been made between the Baltic states and Nordic countries, suggesting that similarities and differences are determined by the respective strategic cultures and can

[26] Kertti Merimaa and Krista Lepik, "Information literacy on the political agenda: An analysis of Estonian national strategic documents," *Central European Journal of Communication* 13, no. 2 (May 2020): 183–201.

[27] Steve Tatham, *The Solution to Russian Propaganda is not EU or NATO Propaganda but Advanced Social Science to Understand and Mitigate its Effect in Targeted Populations* (Riga: National Defence Academy of Latvia, July 2015).

[28] Raquel Miguel, *Towards an Impact-risk Index of Disinformation: Measuring the Virality and Engagement of Single Hoaxes* (Brussels: EU Disinfo Lab, June 2022).

[29] Linton Wells II, "Cognitive-Emotional Conflict: Adversary Will and Social Resilience," *Prisma* 7, no. 2 (2017): 4–17.

[30] Chih-Chien Wang, "Fake News and Related Concepts: Definitions and Recent Research Development," *Contemporary Management Research* 16, no. 3 (2020): 145–174.

[31] "Publications," NATO Strategic Communications Centre of Excellence, last accessed 18 August 2022; "Publications and readings," European Centre of Excellence for Countering Hybrid Threats, last accessed 18 August 2022; "Our work. Research," Baltic Centre for Media Excellence, last accessed 18 August 2022.

[32] Džina Donauskaitė et al., *Baltic Media Health Check 2019–2020. The Media After Covid: Finding strategies to survive and thrive* (Riga/Tallinn/Vilnius: SSE Riga, November 2020).

[33] Volha Damarad and Andrei Yeliseyeu, *Disinformation Resilience in Central and Eastern Europe* (Kyiv: Ukrainian Prism, 2018).

[34] Johannes Voltri, "Comparison of governmental approaches to counter Russian information influence in the Baltic states" (Master's thesis, University of Tartu, 2021).

be characterised in terms of adopted national style, or posture, in countering disinformation. As one such study finds, "in practice, Estonia and Finland have an accommodationist, Sweden – defensive, and Lithuania – offensive strategic culture in their approaches to countering influence activities. Latvia's approach is not so clear-cut, as it admits accommodationist and offensive elements, simultaneously."[35] Thus, while operating in a very similar environment and facing very similar challenges, the Baltic states often employ somewhat different tools and approaches for reaching the same goal – developing a more resilient society.

Nonetheless, a common understanding is growing across the region of the variety of actors that can be involved in posing hybrid threats against the Baltic societies.[36] In addition, various comprehensive overviews of Russia's information warfare and its activities on social media provided some lessons learned, also from the Baltic perspective, on how to effectively counter the malicious online campaigns of the Kremlin regime.[37] This leads to a relatively similar overarching assessment by different clusters of stakeholders in all three Baltic states concerning the well-known long-term vulnerabilities of their societies to malignant foreign influence and effectiveness of long-established policies to mitigate them. Chapter 2 provides an overview of those assessments.

The Baltic states often employ somewhat different tools and approaches for reaching the same goal – developing a more resilient society

2. Status of Known Vulnerabilities and Long-Term Responses

Foreign-led disinformation conducted in the Baltic states usually accompanies malicious influence activities and constructs harmful narratives in certain strategically important areas or sectors, thereby helping to conceal, amplify, or legitimise those activities. It also targets specific vulnerable societal groups, utilises a broad range of instruments and employs both international and domestic actors to propagate those narratives. All this requires tailored cross-sectoral policies and practical measures from the Baltic policymakers and practitioners.

Since restoring independence, each of the Baltic countries have been working to counter disinformation across many sectors by similar, but also different, means. Thus, there is a track record of experience, achievements, failures and shortcomings that forms the backdrop of tackling the emerging new challenges covered later in this report. Before addressing those challenges in the Baltics that emerged during 2020-21, it is important to assess, as a background, the state of play regarding well-known vulnerabilities and existing responses to previously identified problems, or, in other words, 'known knowns.'

This chapter considers the existing perceptions within the five researched clusters of respondents concerning vulnerability and resilience to malicious influence and attendant disinformation in the economic (encompassing such vectors as trade, energy, cyber and technology), socio-political (including civil society and religious organisations) and media sectors. It also captures the assessments and perspectives of those respondents regarding vulnerability of particular societal groups and effectiveness of national responses – conceptual, policy, legal and institutional – to the well-known challenges ('known knowns') in each sector.

[35] Uku Arold, "Põhjala ja Balti riikide psühholoogilise kaitse süsteemide kontseptuaalsed ja praktilised alused [Conceptual and Practical Foundations of the Psychological Defence Systems of Nordic and Baltic States]" (Master's thesis, Estonian Academy of Security Sciences, 2021).

[36] Janne Jokinen and Magnus Normark, *Hybrid threats from non-state actors: A taxonomy* (Helsinki: The European Centre of Excellence for Countering Hybrid Threats, June 2022).

[37] Elina Treyger, Joe Cheravitch, and Raphael S. Cohen, *Russian Disinformation Efforts on Social Media* (Santa Monica, CA: Rand Corporation, 2022).

2.1. Lithuania

In the Lithuanian respondents' opinion, after Russia had launched its aggression Ukraine in 2014, Lithuania was better prepared for malign information attacks than many other European countries when Russia cast serious information operations throughout the continent. Its expertise and proficiency in protecting its information environment, identifying, tracking and neutralising malign topics and themes, and debunking fake news, as well as conducting counter-information and psychological operations, grew rapidly and earned well-deserved respect among Lithuania's allies. Still, each of the reviewed sectors exhibited not only significant progress in mitigating various risks but also contained vulnerabilities that still provided vectors of attack for malign influence and disinformation campaigns.

After Russia had launched its aggression against Ukraine in 2014, Lithuania was better prepared for malign information attacks than many other European countries

2.1.1. Economy, Energy and Cybersecurity

Interviewed respondents unanimously noted that, as of 2020, Lithuania's dependency on economic ties with Russia decreased significantly as Lithuanian businesses successfully diversified their supply chains and export markets, especially since the 2009 global economic crisis. Russia remained an important trade partner, but the top markets for the exports of Lithuanian origin (excluding energy products) were Germany, the Netherlands, the United States, Sweden and other countries.[38] (Lithuania's economic relations with China, that came into sharp focus later, in 2021, were viewed by the respondents mostly in the context of EU-China relations). This has reduced, although not eliminated, Lithuania's exposure to Russia's economic influence and prompted the Russian disinformation efforts to focus on cultivating a narrative of Lithuania being an economic 'basket case' that is completely dependent on the EU's subsidies. Lithuanian respondents noted, however, that the social groups more susceptible to the hostile influence by the Russian state might be entrepreneurs engaged in cross-border activities with Belarus, Russia and those having businesses in the vicinity of the border areas with those countries.

There was a common understanding that by 2020 the main risk of economic vulnerability was related to Russia's interest and efforts to maintain its dominance over the Baltic energy markets. Russian energy companies tried to adapt to new market conditions, based on the market liberalisation and 'unbundling' of infrastructure ownership (following the implementation of the EU's directives) and establish themselves in the Lithuanian gas and electricity markets.[39] This was accompanied by attempts to exert political influence that resulted in high-profile scandals involving members of parliament who allegedly represented Russian energy interests.[40]

By 2020 the main risk of economic vulnerability was related to Russia's interest and efforts to maintain its dominance over the Baltic energy markets

At the same time, Lithuania made significant progress towards strengthening energy independence and security. In 2013, it leased a floating storage and regasification unit (FSRU), *The Independence*, allowing it to import significant quantities of liquified natural gas (LNG) – thus reducing dependence on natural gas imported via pipelines from Russia. Orlen

[38] Economic Complexity Observatory, "Lithuania (trade data)," last accessed 18 August 2022; Viešoji įstaiga Inovacijų agentūra [Innovation Agency Lithuania], "Lietuvos prekių eksporto apžvalga 2021 [Overview of Lithuanian goods export 2021]," 1 March 2022.

[39] State Security Department of the Republic of Lithuania and Second Investigations Department under the Ministry of National Defence of the Republic of Lithuania, *National Security Threat Assessment* (Vilnius: Ministry of National Defence, 2016), 33–34.

[40] Constitutional Court of the Republic of Lithuania, "On the actions of Seimas member Mindaugas Bastys. Conclusion," Constitutional Court, Case no. 12/2017, 22 December 2017.

Lietuva, the operator of the sole oil refinery in the Baltics (owned by Polish PKN Orlen), also pursued successful diversification of crude supplies. In 2015, Lithuania also completed an undersea electricity line to Sweden (NordBalt) and an overland electricity interconnector into Poland (LitPol Link), both of which – in conjunction with the undersea lines between Estonia and Finland – meant that the Baltic states were no longer an energy peninsula abutting Russia. It was expected that Gas Interconnection Poland-Lithuania (GIPL) (that was still under construction in 2020 but became operational in May 2022) would further enhance energy security of the region. It is perhaps an indicator of success of these efforts that malignant disinformation campaigns most arduously targeted, for instance, the FSRU's 'business model' and amplified opposition to this project mounted by the Lithuanian political and business actors still linked to the Russian energy sector.[41]

The issue of ownership in companies involved in national critical infrastructure was perceived as having implications to national security

According to the Lithuanian respondents, as of 2020, the most significant remaining vulnerability in the energy sector was the fact that Lithuania, together with the other two Baltic states, was still part of the Belarus-Russia-Estonia-Latvia-Lithuania (BRELL) set of agreements underpinning synchronous operation of its power grids as part of the IPS/UPS synchronous frequency area managed from Moscow. This vulnerability will persist until Baltic synchronisation with Continental Europe Synchronous Area (CESA) is completed in the end of 2025. It also provides a vector of malignant influence for Russia, including for conducting disinformation operations aimed at obstructing or halting the synchronisation project.

Also, several respondents recalled a particular example of the strategic impact that hostile information operations can have in the energy sector: *"The information campaign against a nuclear power plant (NPP) construction in Lithuania contributed to that Lithuania has not built its own NPP; in the meantime, the Belarusian-Russian Astravyets NPP has been completed and launched."* By the late 2010s, the Astravyets NPP in Belarus, built just 40 km from the Lithuanian capital, came to be seen as a major threat to Lithuania's national security, prompting it to sever electricity imports from Belarus and put pressure on Latvia and Estonia to do the same – thus straining trilateral energy relations.[42] This has further demonstrated that disinformation – in this case targeting the public opinion ahead of the consultative referendum held by the Lithuanian government in 2012 – can have profound and wider-ranging long-term consequences if not dealt with effectively and immediately.

Another security concern voiced by the respondents in 2020 was related to the Port of Klaipėda that had *"closer ties with Russia than the rest of Lithuania"* because *"a few logistics and cargo shipment companies were Russian or Belarusian owned"* and *"Belarus transit cargo went via Klaipėda and Belarus goods production is subsidised by Russia"*. Although the situation has changed significantly since then, given that transit of these goods ceased as a result of sanctions imposed by the EU and the United States on Belarus and, from 2022, also on Russia, the issue of ownership in companies involved in national critical infrastructure was clearly perceived by the respondents as having implications to national security.[43] In connection with this, the respondents underscored the Law on the Protection of Objects of Importance to Ensuring National Security, which contains criteria for assessing the compliance of investors with the interests of national security and is actively applied by the government to screen foreign investments in sensitive economic

[41] Dalia Bankauskaitė, "Propaganda targets Baltic energy independence," *StopFake.org*, 23 January 2018.

[42] Tomas Janeliūnas, "The Long Shadow of a Nuclear Monster: Lithuanian responses to the Astravyets NPP in Belarus," ICDS Analysis, March 2021.

[43] Sanctions were introduced following the fraudulent presidential elections in August 2020 and the unacceptable violence of the Belarus authorities against peaceful protesters, instrumentalisation of migrants for political purpose and hybrid attack at the at the EU's border sanctions and Russia's military invasion of Ukraine on 24 February 2022.

sectors.[44] According to one respondent, it *"sets a framework for economic ties with Russia and China (and any other country) for making such economic relationship less risky"*.

Cybersecurity was high among the issues highlighted by the respondents. The number of cyber incidents in Lithuania as well as globally is increasing every year. The number of cyber incidents recorded by the Lithuanian authorities increased by 25% in 2020 (total 4,330 incidents), while the number of incidents related to the distribution of malicious software increased by as much as 49%.[45] According to the interviewed respondents, the main cyber security challenges were related to the rapid growth of internet-connected devices, the lack of cyber security hygiene and the Soviet infrastructure heritage (in a few cases), whereby *"some IT hardware is from the Soviet period – for instance, train navigation systems – that can still be managed from Russia"*. Strengthening the cyber security environment was, however, viewed as coherent and comprehensive, including inter-sectorial and inter-institutional cooperation and efforts to enhance society's digital literacy.

Russia constantly exploits its country's history to disparage Lithuania's statehood

2.1.2. Socio-Political Aspects

The interviewed respondents stated that Russia constantly exploits its country's history to disparage Lithuania's statehood. The Kremlin furthers the narrative of Russia as the sole victor of World War II (WWII) and also seeks to build a positive image of the Soviet era while discrediting the Baltic anti-Soviet resistance, or the Freedom Fighters – the longest resistance movement in Europe. Strategic communication and security respondents stressed Russia's attempts to promote the myths surrounding WWII and the so-called 'Immortal Regiment' project among Russian-speaking compatriots, especially in Klaipėda but with little success.[46]

There are also attempts to insinuate illegitimacy of Lithuania's current borders. As one respondent noted, *"In the context of the Nagorno-Karabakh conflict, the narrative was pushed forward again that Lithuania owed something to Russia, as its Red Army returned Vilnius to Lithuania."*[47] Some respondents also noted that the regime of Belarus sought to challenge Lithuania's historic narrative: *"Belarus is actively claiming the exclusivity to the Grand Duchy of Lithuania's history."*[48] This also carries connotations of potential territorial claims on Vilnius by Belarus.

Such history-centric narratives, however, were not observed by the Lithuanian respondents in China's attempts to establish itself as an actor of influence in the Lithuanian socio-political domain. According to them, there *"are not many historical parallels with China"* that could be built upon to construct narratives supporting its influence campaigns. However, the Chinese reaction – including through proxies pretending to represent independent societal groups (e.g., the Chinese expatriate community) – is immediately felt whenever the subjects of Taiwan, Tibet or Hong Kong, or of systematic violations of human rights by Beijing are raised in Lithuania as part of principled opposition – both official and from the Lithuanian civil society – to totalitarianism.[49]As for the organisational

The Chinese reaction through proxies is immediately felt whenever the subjects of Taiwan, Tibet or Hong Kong, or of systematic violations of human rights by Beijing are raised

[44] UNCTAD Investment Policy Hub, "Lithuania. Law on the Protection of Objects of Importance to Ensuring National Security," UNCTAD Compendium of Investment Laws, 12 January 2018.

[45] Ministry of National Defence of the Republic of Lithuania, *Nacionalinė kibernetinio saugumo būklės ataskaita 2020 [National Cyber Security Status report for the year 2020]* (Vilnius: Ministry of National Defence of Lithuania, 2021).

[46] Dalia Bankauskaitė, "Disinformation about history leads to disinformation about the present," *Start2Think*, last accessed 18 August 2022.

[47] "Nagorno-Karabakh Conflict: A Visual Explainer," International Crisis Group, 3 August 2022.

[48] "Grand duchy of Lithuania," *Encyclopaedia Britannica*, 9 February 2016.

[49] Dalia Bankauskaitė and Dominykas Milasius, "The Smart Power of Lithuanian Foreign Policy," Center for European Policy Analysis, 27 April 2022.

instruments of Russian influence, Moscow had limited opportunities to advance its agenda in Lithuania through the traditional channels such as the Russian Orthodox Church (ROC). The Russian Orthodox confession is practiced by less than 5% of the population in Lithuania, and therefore its influence in Lithuanian society is rather marginal. The ROC *"keeps low profile, although it has a strong influence among the Orthodox community."* However, some respondents shared their observation that the ROC does engage in politics via its NGOs: "Meloserdie, *a church charity organisation is active both in charity and in domestic politics*". Respondents indicated, however, that the Russian *"GONGOs* [government-organised non-governmental organisations] *network is well established in Lithuania but keeps a low profile. These are entities that act as civil society organisations but, in reality, they carry out destructive activities."* Some respondents pointed out that *"there are fewer GONGOs in Lithuania than in Latvia or Estonia"* that are set up by Moscow.

Susceptibility to disinformation is not based on ethnicity but rather on other socio-political and socio-economic factors

It is important to note that the Lithuanian respondents considered susceptibility to disinformation as not based on ethnicity but rather on other socio-political and socio-economic factors, such as media habits, social 'bubbles', media and information literacy, education and lifestyle. In their opinion, *"the great vulnerability and high threat is the social exclusion"* driven by significant differences in income, quality of education and living standards between different societal groups, as well as by the economic imbalances between the urban centres (especially Vilnius) and the periphery. The Lithuanian respondents indicated that this social exclusion, combined with the 'self-lockdown' in the informational echo-chambers, is very disruptive to the society because *"Russia exploits the societal discontent with the government."* It is this polarised and fragmented environment in which at least some of its malign narratives take root and flourish.

2.1.3. Media Domain

Russian state media had its audience among Lithuania's Russian, Polish and Lithuanian speakers, and it was more popular among older adults who spoke or comprehended the Russian language. The Soviet era nostalgia, however, was not seen as particularly strong among the public, rather *"people feel nostalgic about the time when they were young"*. At the same time, particularly "*Russian-speaking minorities follow Russian state entertainment and news programmes and also watch Belarus national TV and trust them."* Respondents also noted the quality and attractiveness of Russian media entertainment programmes and expressed their wish to see more programmes of high quality to be produced in Russian and Polish languages by the Lithuania media outlets.

Lithuanian respondents noted that social media networks and platforms were extensively exploited by hostile agents to reach out to their target audiences. Virtual gatherings in social media, like online forums and blogs, were often used for the sake of intelligence gathering, provocations, reaction testing and persistent disinformation campaigns. This highlighted that the traditional media focus was clearly insufficient in understanding the dynamics and impact of disinformation activities as well as in countering them.

Virtual gatherings in social media were often used for the sake of intelligence gathering, provocations, reaction testing and persistent disinformation campaigns

The interviewed respondents agreed that, as of 2020, a comprehensive legal framework in terms of detection, prevention and disruption of information threats was in place in Lithuania, and legal procedures for enacting restrictions were clear. The independent media watchdog, the National Radio and TV Commission, actively monitors national information space and is often assisted by a comprehensive network of strategic communication units of state institutions. Representatives of the media, academia and civic society noted that *"the effectiveness of the state regulator (supervisory control of the information to the public) has improved significantly"*. However, they also underlined the risk of political interference, saying that *"the law as such is good, but the politicians constantly try to interfere"*. While addressing *"a subtle balance between freedom of speech and restrictions"*, the respondents suggested that the media regulator be more proactive and have a stronger engagement with the public.

> *The efforts to counter disinformation should be decentralised and based on informal cooperation among state authorities and civil society with mutual trust at the core*

There was a consensus among the respondents that the state also should not do anything that could jeopardise independence and quality of media – a vital element of a democratic society and its resilience, as it is well understood in Lithuania. Assessing the effectiveness of the media code of conduct, the interviewed respondents underlined the long-lasting debate about quality of media reporting and level of journalistic professionalism, as well as about transparency of media ownership and the media business model that provided for the entanglement of political and business interests. Those are significant issues in the national media, but manifest even more in the regions, which is quite detrimental to resilience given "*the importance of quality regional media and reporting from the regions and about the regions*".

Many respondents noted the need for a long-term information strategy for the vulnerable groups in information-poor areas, as *"the need has been evident since 2014, the start of the Russian war against Ukraine."* In addition, there should be more Lithuanian and Western content in the media that are available in ethnic minority languages – the programmes by the national broadcaster in Polish and Russian languages are very well received, but there should be more. Broadcasting licensing in the EU becomes an issue in the cross-border areas. For instance, *"the Polish TV broadcasts to the Lithuanian regions populated by Polish minorities but the re-broadcast of some EU entertainment programs is blocked because of the EU licensing permits, and therefore Polish Lithuanians switch back to the Russian TV."* A few respondents also indicated that the young generation of ethnic minorities used *"the media cocktail of Lithuanian, Russian, Polish and Western social media"*.

The respondents acknowledged that much of the success rested on how the efforts to counter disinformation were organised. They should be decentralised as much as possible and often based on informal cooperation among state authorities and civil society with mutual trust at the core of such cooperation. At least, the media representatives appreciated the effective cooperation with the state authorities in dealing with the challenges of disinformation, even though the overall relations between these two groups of stakeholders were not always without serious complications and difficulties.

Most interviewed respondents highlighted the effectiveness of Lithuania's civil society in countering disinformation but wished the fact-checking that was conducted as part of various civic initiatives would be more comprehensive and included educational aspects. Representatives of the civil society and business sectors also pointed out the importance of the engagement of the whole of society in national security matters and the need to further enhance the skills and knowledge on *"how members of the society could contribute to the information security."* There was a common awareness that the disinformation efforts were moving 'underground' – hence the focus should be on exposing and neutralising various new channels that distribute the Kremlin's narratives. Lithuanian respondents were unanimous in highlighting the need for more in-depth research and applicable policy recommendations, but the fragmentation of research and lack of financing remained significant obstacles to achieving this.

2.2. Latvia

A growing body of literature has examined Russia's influence activities in Latvia. Much attention has been devoted to disinformation and societal resilience-related issues largely because of the Kremlin's activities.[50] Referring to annual public reports of the Latvian security services, including the Constitution Protection Bureau (SAB) and Latvian State Security Service (VDD), it is possible to follow the evolution of influence activities of foreign actors, which currently also includes more information on China.[51] Russia, however, remained the focus and paramount concern of the interviewed respondents when reflecting on Latvia's vulnerabilities and resilience.

> *China and Russia's close intelligence cooperation could mean higher risks for the Baltics in the digital technology domain*

2.2.1. Economy, Energy and Technology

There was no agreement among the interviewed respondents if economic dependence on these two foreign actors – Russia and China – was increasing or decreasing within the studied period. According to the Central Statistical Bureau, exports to Russia from 2020 to 2021 changed insignificantly in the direction of growth. In 2021, Russia was Latvia's fifth main partner after Lithuania, Estonia, the United Kingdom and Germany.[52] At the same time, imports from Russia increased from 2020 to 2021, while gas was the main imported category of goods (approximately €390 million) in 2021.

Energy dependence is one of the main domains mentioned in the context of resilience-enhancing efforts. Respondents from the business sector mentioned that the diversification of energy resources is both a European requirement and a national policy which, for example, resulted in changing of the structure of *Latvijas Gāze* (Latvian Gas), the use of *Nord Pool* electricity market, etc. Transit, port infrastructure and financial operations were mentioned among the topics being used in developing of a 'transit-dependent state' narrative by Russia.

The majority of the interviewed respondents agreed that dependence on China's technology, including everyday products for communication, was increasing. The perception of popularity of social media platforms, applications, games affiliated with Russia or China differed among the respondents of different sectors. *TikTok* and *Telegram* were mentioned among the main and growing platforms. Both are problematic from the point of view of monitoring malignant influence activities. Interviewed Latvian government representatives were concerned about the dependence on China's technologies on the everyday level: "*People buy the cheapest product, without taking into account the warnings.*" A few media representatives mentioned the case of phones and video surveillance equipment installed for the purposes of spying on a building situated near the Latvian Ministry of Defence.[53] Another case was the plans to install Russia-related equipment near the Alūksne military base.[54]

Awareness among the general public in Latvia concerning the risks of dependence on the Chinese technology was evaluated by the security and defence sector representative as rather low. Some respondents pointed out that China and Russia's close intelligence cooperation (referring to the interviews

[50] Artis Pabriks and Andis Kudors (eds.), *The War in Ukraine: Lessons for Europe* (Riga: University of Latvia Press, 2015); Andis Kudors (ed.), *Fortress Russia: Political, Economic, and Security Development in Russia Following the Annexation of Crimea and its Consequences for the Baltic States* (Riga: The Centre for East European Policy Studies, University of Latvia Press, 2016); Māris Cepurītis et al., *Russia's Footprint in The Nordic-Baltic Information Environment* (Riga: NATO Strategic Communication Centre of Excellence, 2018).

[51] Constitution Protection Bureau of the Republic of Latvia, *Annual Public Report of the Constitution Protection Bureau of the Republic of Latvia (SAB)* (Riga: Constitution Protection Bureau, 2021).

[52] Central Statistical Bureau of the Republic of Latvia, *Latvijas ārējā tirdzniecība. Svarīgākās preces un partneri 2021. gadā [Foreign Trade of Latvia: Main Commodities and Trade Partners, 2021]* (Riga: Central Statistical Bureau, 2022).

[53] "Nekā personīga" news story quoted from: "Valsts iestāžu darbinieku tālruņi slepus sūtījuši datus uz serviertem Ķīnā [Phones of Latvian public servants have been secretly sending data to servers in China]," *la.lv (Latvians News)*, 28 November 2016.

[54] "Krievija gribējusi ierīkot novērošanas kameras ap Alūksnes ezeru. Tas ļautu izspiegot blakus esošo armijas bāzi [Russia wanted to install surveillance cameras around Lake Alūksne. This would enable to spy on a nearby military base]," *TV3.lv*, 31 May 2020.

conducted in 2020) could mean higher risks for the Baltics in the digital technology domain.

Some business sector respondents underlined that, within the critical infrastructure sector, the awareness of national security threats posed by Russia and China was high. During 2020-21, procedures for ensuring conformity of information and communication technologies systems to the minimum-security requirements were revised with amendments in 2017, 2019 and 2020.[55] Yet concerns remained about the ability to buy gadgets for kids and families, routers etc. – where Chinese products are available for the lowest price, especially for younger members of families (one of the most vulnerable groups). The business cluster representative also pointed out the significant budget that China was devoting to the Baltic market for promoting technologies. As an example, the interviewee mentioned increased visibility of Chinese *Huawei* campaign both as ordinary and native advertisement in Latvian online media, even though this campaign decreased significantly due to the COVID-19 pandemic.

Banning users and taking out the content on popular social media platforms motivated some groups to find other places to exchange their provoking or disinforming views

Respondents generally agreed on the fact that the number of cyber threats was increasing. The annual report by the SAB, however, stated that the number of foreign cyber-attacks had remained stable for the last 4-5 years at the level of several tens of thousands of attacks each year.[56] Furthermore, when asked to elaborate, the interviewed respondents had difficulties naming specific cases. Therefore, general awareness was more connected to international trends, and it was hard for the majority of the interviewed respondents to recall any known cases from Latvia. Some respondents referred to good cooperation with the Computer Emergency Response Team Latvia (CERT.LV). Respondents working with the critical infrastructure mentioned well-trained staff and increasing general awareness. At the same time, journalists and civic actors would benefit from knowing more on the tactical objectives of cyber-attacks as well as adapt to the terminology used.

Council Regulation (EU) 2019/796 of 17 May 2019 concerning restrictive measures against cyber-attacks threatening the Union or its Member States served as an additional set of actions to protect cyberspace. While cyber-incidents were traditionally treated in a quantitative manner, sharing qualitative data on actors, aims and transmission mechanisms was needed for understanding and countering influence campaigns (as a part of cognitive warfare). As underscored by the interviewed information security related respondents from the business cluster, a special focus should be set on raising the awareness of the vulnerable audiences as to their potential targeting for intelligence-gathering and cognitive influence.

Awareness of the general public concerning information security and cyber threats was perceived as mixed. "*Do they see why they have to protect data*?" a government related respondent posed a question without giving an answer. Think-tank representatives pointed out the need to increase awareness on the use of big data in general, even when the individual "*has nothing to hide,*" and how this data could be used and what possibilities for microtargeting were being provided to malignant actors.[57]

Forums and other views-exchange platforms (apart from social media) were also evaluated differently. The view expressed by several respondents was that banning users and taking out the content on popular social media platforms motivated some groups to find other places to exchange their provoking or disinforming views without risks. *Imhoclub.lv*, according to government-related respondents, was one of the most popular

[55] Cabinet of Ministers of the Republic of Latvia, "Kārtība, kādā tiek nodrošināta informācijas un komunikācijas tehnoloģiju sistēmu atbilstība minimālajām drošības prasībām [Procedures for the Ensuring Conformity of Information and Communication Technologies Systems to Minimum Security Requirements]," Likumi.lv (Legal Acts of the Republic of Latvia), 28 July 2015.

[56] Constitution Protection Bureau of the Republic of Latvia, *Annual Public Report.*

[57] Samantha Bradshaw and Philip N. Howard, *The Global Disinformation Order. 2019 Global Inventory of Organised Social Media Manipulation* (Oxford: University of Oxford, 2019).

Tensions between conservative and liberal political organisations in Latvia were named as a gap used by the Kremlin

platforms. In previous public reviews, Latvian security authorities named the forum as Russia's employed project. Respondents also mentioned other niche forums for communities (possible target audiences) – such as sport-fans, parents, mothers – pointing out the risks of low monitoring, lack of self-regulating and informationally easy to penetrate which also points to broader socio-political aspects at play.

2.2.2. Socio-Political Aspects

In perception of the interviewed respondents, the Kremlin's activities and interests were built around multi-dimensional questions. Besides the economy and finances, there were culture and education (emigration to Russia to study, import and advertisement of education products), values and beliefs (with the focus on traditional values), history, etc. Several respondents also emphasised that any electoral campaign used questions to mutually benefit pro- and anti-Russian agendas. There were respondents in each sector who mentioned that some local political initiatives were helpful to the Kremlin. Civic activists and opinion-leader cluster representatives shared a view that some of these issues were used by local politicians as a mobilisation tool for the domestic electorate.

Tensions between conservative and liberal political organisations in Latvia were named as a gap used by the Kremlin, as pointed out by civic activists. At the same time, no significant intensification in this regard had been observed by respondents: "*We are not as interesting to Russia as other neighbours. They do not invest financially but are mainly using our mistakes and use low-cost methods. We deliver these topics to them by ourselves.*"It was widely recognised that one of the Kremlin's goals was to divide societies in Europe.[58] In Latvia, according to the majority of the interviewed respondents, this took place by decreasing the sense of belonging to Latvia among the so-called compatriots and by spreading general distrust to the public institutions, including the media. Trust of information sources was also an important issue when dealing with disinformation.[59] Some government-related respondents mentioned that several influence agents were being used to make appearances in the media by organising protests and other activities. Any mistake in governing the state was exploited, including accusing Latvia of being a non-democratic state.[60]

Most of the interviewed respondents shared the view that the influence of the Russian Orthodox Church (ROC) had decreased within the studied period. One of interviewed respondents mentioned that the Latvian Orthodox Church became more independent from the Moscow Patriarchate. In September 2019, an amendment was introduced in the law of the Latvian Orthodox Church stating that the candidates for the Head of the Church should have permanently resided in Latvia for no less than ten years.[61] According to one of the respondents, the initiative to adopt this amendment came from the representative of the church. The same interviewed respondent connected it to the personality of the current Head of Church and warned of possible changes in the case of personnel turnover. Another relevant issue pointed out by the academia representatives was that there was not enough data on the mood of Orthodox believers, including the attitudes of the old-believers.[62] When asked to name and evaluate hostile information operations directed against Latvia's interests, the most commonly mentioned cases were about NATO's presence in Latvia (military exercises, Enhanced Forward Presence, NATO

[58] Edward Lucas, Ben Hodges, and Carsten Schmiedl, "Close to the Wind: What Russia Wants," Center for European Policy Analysis, 9 September 2021; Geir Hågen Karlsen, "Divide and rule: ten lessons about Russian political influence activities in Europe," *Palgrave Communications* 5 (8 February 2019).

[59] Ieva Bērziņa, "Political Trust and Russian Media in Latvia," *Journal on Baltic Security* 4, no. 2 (December 2018): 1-8.

[60] Foundation for European Progressive Studies, *Resisting Foreign State Propaganda in the New Information Environment: the Case of the EU, Russia, and the Eastern Partnership Countries* (Baloži: Foundation for European Progressive Studies, Brīvības un Solidaritātes Fonds, 2016).

[61] Saeima, "Latvijas Pareizticīgās Baznīcas likums [The law of the Orthodox Church of Latvia]," Likumi.lv (Legal Acts of the Republic of Latvia), 3 December 2008.

[62] According to Central Statistical Bureau, there were 72 congregations of old-believers in 2020, see: Central Statistical Bureau of the Republic of Latvia, "Registered religious congregations by denomination at the end of year 1990-2020," Official statistics portal, last accessed 18 August 2022.

Strategic Communication Centre of Excellence, etc.); historic issues, including Remembrance Day of the Latvian Legionnaires (16 March) and other history related dates; Latvian authorities and personalities (e.g., a book about the president Egils Levits);[63] the economy and financial system (sanctions, banks and money laundering, blacklisting of the suspended former Mayor of Ventspils, Aivars Lembergs, etc.); topics related to the construction of *Nord Stream* undersea gas pipeline by Russia and the *Rail Baltic* railway project.

The lack of political will was mentioned among the main problems in increasing the effectiveness of the state's long-term approach towards vulnerable groups

Some Latvian respondents distinguished between calendar-based and surprising information activities. Respondents also pointed out difficulties in tracking such operations, as there were ongoing long-term operations with active and passive phases. Terminology made it difficult to call some activities an operation. One respondent shared a view that they were frequently "*not seeing a flower, but smelling it,*" as tools and channels were constantly changing, and micro-targeting was being used in such operations.

The lack of political will was mentioned among the main problems in increasing the effectiveness of the state's long-term approach towards vulnerable groups. Inability to reach and engage the audience due to specific channels and language among vulnerable audiences were mentioned in addition to the lack of resources. At the same time, the government-related respondents noted that the level of awareness among the institutions and politicians on the need for a long-term approach was increasing. The need for an asymmetric response was also mentioned in order to protect these audiences.

Respondents from the government and think-tank/academia clusters mentioned difficulties associated with strengthening security while upholding democratic values. The discussion of prohibiting various tools of influence and the connotations of censorship that this entails was not unique to Latvia. One respondent pointed out the risks of inconsistencies in banning and deleting procedures for the online content while seeking to ensure the freedom of expression. The interviewed representatives therefore disagreed when evaluating the bans on the Russian media implemented by the Latvian regulator.[64] Yet, there was general awareness that democracy had to be protected against disinformation.[65]

A majority of the respondents from all clusters mentioned the increasing number of research on audience and disinformation. At the same time, those dealing with research (the academia and think-tank cluster), as well as their clients (the governmental cluster) mentioned that the local research was still under-financed, frequently limited with quantitative surveys and lacking qualitative analysis. A respondent involved in disinformation monitoring pointed out the lack of general strategy in Latvia: "*So far it looks like groping, showing average temperature. Reports are mainly showing tendencies, not going deeper inside, but it is normal as it is only an emerging area.*" Some other interviewees mentioned the risks of limitation of the research without multidisciplinary aspects, connectivity and ability to develop the needed research apparatus to address changes in media consumption.

[63] For more details see: "Levits komentē Lato Lapsas grāmatā "Viltvārdis" izteiktās šaubas par viņa biogrāfiju [Levits comments on the doubts expressed in Lato Lapsa's book "Viltvārdis" about his biography]," *Apollo.lv*, 16 July 2020.

[64] In July 2020, the Council banned RT due to control over it by D. Kiselyov, who is on the EU sanction list, see: National Electronic Mass Media Council of Latvia, "NEPLP: Kiselyov, who is on the EU sanction list, ensures full control over RT according to the decree signed by Putin," 7 July 2020. In February 2020, the Council decided to ban distribution of nine programmes: "Vremya: dalekoye i blizkoye" ("Время: далекое и близкое"), "Bobjor" ("Бобёр"), "Dom Kino" ("Дом Кино"), "Dom Kino Premium" ("Дом Кино Премиум" / "Дом Кино Premium"), "Muzika Pervogo" ("Музыка Первого"), "O!"("O!"), "Poyekhali" ("Поехали!"), "Telecafe" ("Телекафе") and "Peterburg – 5 kanal" ("Петербург - 5 канал"). It was justified by information received from the VDD about connection of these programmes to Jury Kovalchuk, who is under sanctions in the EU due to Russia's activities in Ukraine, see: National Electronic Mass Media Council of Latvia, "The court decides to maintain the NEPLP decision on restricting the distribution of 9 programmes," 12 February 2020.

[65] Tarlach McGonagle, Maciek Bednarski, Mariana Francese Coutinho, and Arthur Zimin, *Elections and Media in Digital Times* (Paris: UNESCO, 2019).

2.2.3. Strategic Communications and Media Domain

There was no agreement among the interviewed respondents on the evaluation of institutional development in the sphere of information security in Latvia. Interviewed media representatives provided more negative evaluation, while others were more positive about efforts of different governmental and non-governmental actors. The general idea shared by respondents was that, within the studied period, awareness on disinformation had increased at many levels.

Establishment of the State Chancellery's Strategic Communications Coordination Department was the most frequently mentioned achievement. This institutional body was the first steppingstone in developing the necessary structure and cross-sectoral coordination. The governmental office of StratCom also provided access to monitoring tools and training to use these tools. The new body significantly increased the number of trained civil servants. The Latvian State Chancellery was also the contact point for Big Tech companies (i.e., Google, Facebook, Twitter), but had not tried reaching the Russian social media platforms such as *VKontakte* (VK) or *Odnoklassniki* (OK) as of 2021. In the evaluation of such cooperation, government and media related representatives shared the view that respect for the state authorities shown by these Big Tech companies was usually higher than for single actors such as journalists or independent experts.

Increasing strategic communication staff and departments in the government's ministries was mentioned as another successful measure. Think-tank and academia respondents underlined significant efforts of the Latvian Ministry of Defence at the level of planning and regulatory documents that brought an information environment into defence and security agenda.[66] The cognitive dimension of resilience was actualised in the legal framework, paying more attention to psychological resilience. The Latvian Ministry of Foreign Affairs increased its capacity by restructuring divisions and creating a post of special envoy on information security. Representatives of the governmental sector also positively highlighted the multidisciplinary teams, as well as exchange of staff with international structures (EU StratCom Task force, NATO Strategic Communication Centre of Excellence, EU Hybrid CoE, etc).

Some government cluster's respondents referred to evidence of increased ability to mobilise staff in key ministries (Ministry of Defence, Ministry of the Interior, Ministry of Foreign Affairs), pointing also to increased staff training. For engagement with the civil society, media and governmental sector, the respondents mostly named other institutions – including think-tanks, NATO Strategic Communication Centre of Excellence and the Baltic Centre for Media Excellence. While NATO Strategic Communication Centre of Excellence is an organisation for international cooperation, it also serves as a platform to increase understanding of ongoing processes and builds awareness domestically. The staff of the Centre participate in different capacities in national initiatives, bringing a hands-on approach to developing informational security. Some of the mentioned examples were advising the government, providing updates on trends in disinformation and misinformation, training and public appearances. The Baltic Centre for Media Excellence, in addition to enhancing qualitative journalism and media literacy, served as a hub for ensuring election integrity and provided networking for stakeholders such as journalists and think-tankers. Both organisations had attracted the Kremlin's attention and had been targeted in disinformation activities against them.

There was no agreement among the interviewed representatives on evaluating the level of comprehensiveness of the legal framework for detection, prevention and disruption of information threats and vulnerabilities. The most common example mentioned was the case of the owner of several quasi-news portals, Niks Endziņš.[67] A media-related respondent mentioned that most detected and discussed cases in Latvia were so-called commercial fakes where the main aim to earn money is with clicks (clickbait). A few respondents remembered the discussion on the need for revision of the Criminal Law, which was not fruitful as of 2021.

[66] Ministry of Defence of the Republic of Latvia, *Valsts Aizsardzības Koncepcija [State Defence Concept]* (Riga: Ministry of Defence, October 2020).

[67] Liene Barisa-Sermule, "Fake News kingpin kept behind bars," *LSM (Latvian Public Broadcasting)*, 7 September 2018.

While some respondents unrelated to media shared the view that efficient media monitoring systems were in place, failure of detection of disinformation by journalists remained a high risk. Interviews with media representatives showed that journalists who were not fact-checkers did not have access to monitoring platforms and were not trained to use them. There was a clear need to increase the availability of monitoring software, additional general and tool-specific knowledge and skills to be trained regularly on the use of tools for journalists.

Failure of detection of disinformation by journalists remained a high risk

The respondents working with monitoring tools named certain problems connected to the process of data gathering. Some were related to the Latvian language (declinations/forms) and design of tools: "*for example CrowdTangle, if you see quite popular page in Latvia, but tiny comparing to other world's pages, you are adding it to data base only when it has been noticed.*" The search option in this type of tools was not elastic to the Latvian language, as it was mentioned by the respondents. At the same time, some think-tanks and academia-related respondents were working with these tools, but they struggled to create audience-friendly texts.[68]

The Latvian respondents disagreed on the effectiveness of media community regulation. There are two main organisations for journalists and several media-related associations in Latvia. Think-tanks and academia, as well as several opinion leaders, mentioned that the community was fragmented. This fragmentation was not ethnic or linguistic, but rather into professional 'bubbles' and along the lines of media ownership. It was quite common for the Russian language journalists to not be part of any professional journalistic organisation.[69] Russian language products, as mentioned by one of the respondents, rarely were in the focus of, for example, journalism award-giving competitions in Latvia, while the Russian Embassy has had an award dedicated for this target group for more than a decade.[70] This award was also mentioned in the reports of security services.[71]

Several interviewed respondents mentioned the creation of the Latvian Media Ethics Council in December 2018 among the positive steps.[72] The interviewed respondents shared some concerns on the ability of this organisation to improve the media environment: "*Good that the Council exists, but it is hard to evaluate its authoritativeness and effectiveness so far.*" Besides the above-mentioned Baltic Centre for Media Excellence, there was the Media Centre in Riga Stockholm School of Economics that also organised events to strengthen qualitative journalism. The centre also founded the Peter Greste Baltic Freedom of Speech Award, the school on investigative journalism and supported the media environment study *Baltic Media Health Check*.[73] Another concerning issue identified by the respondents was the non-transparency of ownership of key media companies, as well as the shrinking advertisement market because of the marketing budgets being redirected to the social media platforms.

Regarding the main regulatory authority, the National Electronic Mass Media Council – which in Latvia is dedicated solely for the electronic media, the respondents voiced their main concerns regarding its mixed responsibility for commercial and public service media and the role of politicians in the process of forming the council elected by the Latvian parliament, Saeima. Both questions were addressed in the new media legislation adopted by Saeima in November 2020 that came into force on 1 January 2021. The newly formed Public Electronic Mass Media Council (SEPLP) consists of three members – one delegated by the President, one by the Saeima

[68] Solvita Denisa-Liepniece and Dmitri Teperik, "Local Russian-language Journalism in the Baltics: Challenges and Perspectives for Building Resilient Communities of Media Professionals," ICDS Policy Paper, March 2022.

[69] Ibidem.

[70] Russian Federation Embassy in Latvia, "Mezhdunarodnyj konkurs sredi zhurnalistov "Yantarnoye pero" [Amber Feather Journalism Competition]," last accessed 18 August 2022.

[71] Latvian State Security Service, *Annual Report on the activities of Latvian State Security Service in 2019* (Riga: Latvian State Security Service, March 2020).

[72] "Latvijas Mediju ētikas padome - dokumenti [Latvian Media Ethics Council - documents]," Latvian Media Ethics Council, last accessed 18 August 2022.

[73] Stockholm School of Economics in Riga, "Baltic Media Health Check 2018-2019 published," SSE Riga, 5 November 2019.

and one by the Council of the Implementation of the Memorandum of Co-operation between NGO and the Cabinet. In December 2021, Anda Rožukalne was elected as the first public media ombudsman. According to the interview with a government sector representative, changes in European legislation may lead to an increased monitoring function of the Council, including on social media.

The government instituted a set of institutional responses, supplemented by civic and private sector initiatives and platforms, that provides a robust framework for addressing cyber threats

2.3. Estonia

Russian and, increasingly, Chinese malign influence activities targeting Estonia, as well as the country's efforts to build resilience against them, have been continuously highlighted by various research studies and annual reports by the security and intelligence services.[74] Thus, the sample of interviewed respondents had a well-established mental map of the nature and severity of the threats, including disinformation.

2.3.1. Economy, Energy and Cybersecurity

The majority of the interviewed respondents assessed the Estonian economy to be EU-focused and its dependence on Russia and China was considered rather small. That can be explained by the fact that, since the basic principles of the export policy adopted in 2001, Estonia has been striving towards "economically and politically stable trade partners" to lower the risks.[75] After Russia's aggressive actions against Ukraine began in 2014, Estonia's major exporters expanded their target countries to another 14 countries to spread the risks, and today Estonia's top five trade partners are Finland, Sweden, Latvia, the USA and Germany.[76]

However, due to geographical proximity to Russia, energy risks remained, especially in the field of electricity. As noted by one of the respondents:

> *Trade with Russia regarding energy is remarkable, starting with oil, natural gas and electricity, but there is no dependence, as they are traded according to world market rules and therefore there is a substitution. Situation with gas is a bit more complicated but no dependence either as there are alternatives. The situation is most difficult when it comes to electricity because there has been no desynchronisation from the Russian network.*

Nevertheless, this problem is already being solved and according to the current plan, at the end of 2025 the Baltic states should leave the Integrated Power System/Unified Power System (IPS/UPS) grid of Russia and join the CESA.[77]

Estonian respondents also pointed out that although direct trade with China was not large, there was still certain dependence through the EU as a whole, for China is the EU's second most important trading partner after the US.[78] In addition, the interviewed respondents have noted as a more well-known issue that, in the Estonian business community, sometimes business interests and profit opportunities outweigh risk awareness.

Due to Estonia's experience of cyberattacks in 2007 and the whole-of-government and whole-of-society approach adopted by the national Cybersecurity Strategy of 2008 (as well its subsequent iterations), the interviewed respondents pointed out that the level of awareness of cyber-threats in the society is relatively high. The government itself also instituted a set of institutional responses, supplemented by civic and private sector initiatives and platforms, that provides a robust

[74] "Aastaraamatu väljaandmise traditsiooni ajalugu ja eesmärk [Annual reviews: History and Goals of the Tradition of Annual Reviews]," Estonian Internal Security Service, last accessed 18 August 2022; "Security environment assessment," Estonian Foreign Intelligence Service, last accessed 18 August 2022.

[75] Riigikogu, "Eesti ekspordipoliitika põhialuste heakskiitmine [Approval of the principles of Estonian export policy]," *Riigi Teataja,* RT I, 92, 556 (2001).

[76] "Estonia: Destinations 2021, Consignment 2021," Statistics Estonia, last accessed 18 August 2022.

[77] Hannes Kont, "Synchronization with continental Europe," Elering, updated July 2022.

[78] "EU27 Trade in Goods Services by partner (2020, excluding intra-EU trade)," European Commission, Directorate General for Trade, last updated 20 April 2022.

framework for addressing these threats. For instance, in 2009, a Cyber Security Council was established as part of the Government's Security Committee, with the goal of "contributing to smooth co-operation between various institutions and conduct surveillance over the implementation of the goals of the Cyber Security Strategy".[79]

> *The effects of urbanisation within Estonia and the spreading perceptions of Ida-Virumaa as a regional ghetto contribute to the effectiveness of disinformation*

Their work is in turn facilitated by the Information System Authority (RIA) and the Government Office.[80] RIA's annual cybersecurity reports facilitate greater awareness across the state and society about the state of play in this field, while a handbook by e-Governance Academy provides a set of tools to national cybersecurity practitioners working, among many other directions, to ensure resilience to the attempts to exploit the cyber domain for malign influence activities.[81]

2.3.2. Socio-Political Aspects

All the interviewed respondents acknowledged the persistent problem of the constant twisting of history and presentation of alternative facts by Russia. Commonplace narratives include considering Estonia as a part of Russia since the 18th century, denying the occupation by the USSR and amplifying the problems of the North-Eastern Estonian region (Ida-Virumaa). The latter is pursued through strategically placed and ideologically motivated moves and messages designed to keep the Russian speaking minority divided from the main society by criticising Estonian citizenship policy, spreading Russian identity through the ROC or by popularising and romanticising the USSR-era imperialist mentality, lifestyle, monuments and celebrating various chauvinist memorials during the so-called Victory Day of 9 May. As noted aptly by one of the interviewed respondents: "*all the major problems that exist in society can be used to shake the stability of society*".

The effects of urbanisation within Estonia and the spreading perceptions of Ida-Virumaa as a regional ghetto contribute to the effectiveness of such disinformation. However, receptiveness to disinformation is not confined to this region alone.[82] Estonian respondents pointed out the lack of regional policy and rapid urbanisation as old challenges which in turn cause problems in small towns and rural areas such as reduced prospects for a better future, low wages, lower travel opportunities, etc., making them more vulnerable to disinformation. The lack of political consensus in the field of education and integration was also pointed out as an old systemic problem, which in turn has not helped to solve the problem of the availability of education and language training in the Estonian language in Ida-Virumaa and other areas: "*Polarisation and radicalisation in Ida-Virumaa is not so bad, perhaps it is even bigger in Tallinn. Rather, the problem is that there is no opportunity to speak Estonian, however there is a positive attempt*."

Regarding the visible activity of GONGO's or other agents of malignant foreign influence in Estonia, the majority of the interviewed respondents assessed it as small or very small. Some respondents mentioned organisations such as the Centre for Human Rights, NGO Russian School in Estonia, NGO Estonian Indo-European Union and Estonian Left Party, which have been noticed to spread a strategic agenda that can be related to Russia under the name of fighting for human rights or education equality. However, their impact is assessed to be small in general. When it comes to Estonian political parties, some topical overlap with the Kremlin's narrative and agenda was pointed out, but no direct connections have been identified.

[79] "Riigi küberturvalisuse tagamine [Ensuring Cybersecurity]," Ministry of Economic Affairs and Communications of the Republic of Estonia, last accessed 18 August 2022.

[80] "Strategic communication," Government Office of the Republic of Estonia, last updated 8 February 2022; Epp Maaten and Toomas Vaks (eds.), *National Cyber Security in Practice* (Tallinn: E-riigi Akadeemia, 2020).

[81] "Publications – Yearbooks," Information System Authority of the Republic of Estonia, last accessed 18 August 2022; Maaten and Vaks, *National Cyber Security in Practice*; "Meediapädevuse nädal 2020 [Media Literacy Week 2020]," Ministry of Education and Research of the Republic of Estonia, last updated 16 February 2021.

[82] Dmitri Teperik, "Democracy, 'Alternative Reality' and Estonia's Resilience," ICDS Brief, October 2020.

2.3.3. Media Domain

Media controlled from abroad play an important role in transmitting the Kremlin's narratives in Estonia. Due to its geographical proximity, history and popularity among the local Russian-speaking minority, the Russian media stood out. Some respondents also mentioned China's channels broadcasting in English – cctv.com, for example – however, their popularity in Estonia remained very small.

> *Viewers were attracted to the Russian media mainly due to entertaining content, easy accessibility and a lack of alternatives*

Although the majority of the Estonian population considered the Russian media unreliable, there was still a fragmented group of people who followed it for various reasons. According to the interviewed respondents, these people were usually united by their limited knowledge of the Estonian language that, in turn, resulted in further problems such as limited access to higher education, limited opportunities in the labour market and reduced access to the Estonian information space all of which made them prone to disinformation. As one respondent pointed out, regardless of the reasons and extents to which a person monitored the media that transmitted disinformation, the distorting effect could be still noted.

Viewers were attracted to the Russian media mainly due to entertaining content, easy accessibility and a lack of alternatives. According to a previous survey, Russian channels such as PBK and its "Novosti Estonii" as well RTR Planeta and its "Vesti" were still considered to be rather reliable by the Russian-speaking audience of Estonia as of 2020. However, the main news show of the Russian language channel ETV+ (part of the public broadcaster ERR) has grown to become the most reliable news programme among the Russian-speaking population.[83] This further highlighted the importance of trustworthy and objective local and national news sources broadcasting in languages of the target audiences.

The interviewed respondents, however, have pointed out the lack of co-operation, fragmentation and slow dissemination of information between the services and organisations dealing with disinformation countering, which makes the process not as efficient as it could be. Overall coordination is in the hands of the Government's Office and its Strategic Communications Unit, but various ministries and government agencies that traditionally are rather independent in executing their mandates usually have their own agendas or even ignore the need for a coherent long-term approach to countering disinformation, especially among the Russian-speakers and in various vulnerable societal groups.

> *The lack of co-operation, fragmentation and slow dissemination of information between the services and organisations dealing with disinformation countering makes the process not as efficient as it could be*

Nonetheless, the respondents highlighted some important endeavours to enhance society's resilience to disinformation. Some recent examples mentioned by the respondents included media literacy week and media and communication activities in schools and in the media to raise awareness of the disinformation problem. Furthermore, this awareness was constantly developed through various educational programmes aimed at enhancing society's understanding of national security and defence, such as the National Defence Course for the schoolchildren at the upper secondary schools, educational activities of the Estonian Defence Forces and also through the Higher National Defence Courses organised by the ICDS.[84] There were also programmes

[83] Marju Himma, "Uuring: ERRi usaldusväärsus kasvab, eriti vene inimeste hulgas [Survey: trust in ERR is growing, especially among Russian people]," *ERR*, 31 May 2019.

[84] "Estonian National Defence Course (ENDC)," International Centre for Defence and Security, last accessed 18 August 2022.

within the ministries conducted with a primary goal, established by the Government Office, to equip each ministry and their subdivisions with at least one expert in the field of counter-disinformation.[85]

3. Preparing Societies for New Challenges

The accelerating geopolitical, societal and technological change that is punctuated by ever more frequent crises means that the Baltic states could not afford standing still in their efforts to strengthen their national resilience. Indeed, since the completion of the first round of the interviews for this report in 2020, they found themselves in the midst, or even at the forefront, of crises and confrontations that were just passingly featured in their security assessments and threat perceptions prior to 2020-21.

Economic ties with China emerged as a vector of influence in the business community of Lithuania and as a tool of political coercion

As the COVID-19 pandemic engulfed the world, the Baltic societies went through similar societal, political and economic turbulence as many other countries – turbulence that was amplified and exploited by malignant disinformation campaigns and foreign interference. Lithuania and Latvia also faced an illegal migration and border security crisis engineered by the regime in Belarus that also overlapped with the riots against the governments and their pandemic management measures and, in the case of Lithuania, came on the heels of a crisis triggered by the hijacking of a Vilnius-bound *Ryanair* passenger flight by the Belarusian authorities. Last but not least, Lithuania found itself at the sharp end of China's economic and diplomatic coercion, as well as a propaganda assault, due to the opening of the Taiwanese representation office in Vilnius.

All of this, while not fundamentally altering the overall landscape of threats and vulnerabilities or triggering entirely new institutional or policy responses, has nonetheless dramatically changed the context in which those risks and responses are playing out. In addition to testing national resilience, they are also triggering tentative reassessments of the new and old gaps and rethinking ways forward. This chapter presents the views of the interviewed respondents concerning the developments that challenged security and resilience of the Baltic states in 2020-21, before the onset of an even more tumultuous and dangerous year 2022.

3.1. Lithuania

Although the challenges and risks to societal resilience on the strategic level remained the same, the changing geopolitical situation on the operational level made certain security aspects more urgent. Many interviewed respondents noted that Russian and Belarusian propaganda activities against Lithuania have intensified. Pro-Kremlin political marginals living in Lithuania are often used for this purpose. Russian and Chinese intelligence services are actively spying in cyberspace. Interviewed respondents underlined Lithuania's success in policing and monitoring the information space, but also noted that building societal resilience is a multidimensional and strategic challenge that requires a comprehensive and consistent approach.

3.1.1. Economy and Technology

Economic ties with China came to the forefront of attention in Lithuania in 2021, as the country wrestled with a harsh response from Beijing to the opening of the Taiwanese diplomatic office in Vilnius. These ties emerged both as a vector of influence in the business community of Lithuania and as a tool of political coercion. The respondents shared the opinion that Lithuania's economic relations with China should be assessed in the EU context: *"As the Chinese lobbyism is very strong in the EU, it is also felt in the Baltics. Lithuania's dependency on China is indirect"*. On the other hand, the interviewed business representatives also noted that China's pursuit of technological advantage and its penetrating investment activities increase the vulnerability and pose the risk of losing

[85] Ibidem.

control over the critical infrastructure of the country. Business representatives voiced their concern that the EU might soon lose its competitive advantage and capabilities against China: *"The EU does not protect their industries and give preference to the access to the Chinese market"*.

Respondents stressed the importance of a long-term integration and inclusion programme for ethnolinguistic groups as well as the new immigrants

In respondents' opinion, Lithuania's dependency on Russian and/or Chinese communication and/or IT-related technologies remains rather high although manageable. At the same time, as noted by several respondents, *"the scope of cyber-attacks is growing as well as their complexity. There are too many attacks for such a small country like Lithuania."* The greatest threat to the security of Lithuanian information systems and the information stored in them comes from the cyber espionage conducted by the Russian intelligence services. The development of 5G technologies may become a new risk factor if the necessary attention is not paid to the reliability of the provider of information technology services or products.[86] Respondents noted that cyber-attacks usually go together with information operations. The good sign is that the awareness keeps growing among state institutions, businesses and the public concerning digital security. State institutions regularly review their IT technologies and equipment procurement policies. However, the cost of technology influences their decisions, while there is "*the risk arising at the EU level, as it pays too little attention to what IT products get into the EU market*".

Concerning the potentially malignant influence through trade, payment, or investment, the respondents underscored the importance of diligent scrutiny of money origin and business ownership in order not to become a convenient place to land for sanctioned businesses from Belarus and Russia. Lithuanian respondents pointed to the political will at the national level and understanding within the society on the necessity to withstand Russia's and China's economic lobbyism and the need to prioritise the country's competitiveness over the short-term business gains. Business community representatives repeatedly stressed the importance of comprehensive cooperation with state institutions, particularly national security agencies, in ensuring compliance of the major economic, technology and innovation programmes and foreign investors with national security interests.[87]

3.1.2. Society, Politics and Media

The COVID-19 pandemic health crisis was viewed by interviewed respondents as a challenge from the point of crisis management and political leadership skills. Disinformation and framing of malign narratives by hostile actors increased the risks of societal fragmentation and polarisation because, at the initial stage of the pandemic, the proactive sense-making of the crisis by the government was slow or even non-existent. Interviewed respondents classified the circulating narratives as enhancing geopolitical, economic and technological confrontation. These malign narratives were about the pandemic conspiracy, carrying anti-EU and anti-NATO, anti-vaccine and anti-vaccination messages. On the other hand, several Lithuanian respondents noted the inconsistency of Russian propaganda – initially, Russia's media furthered narratives denying the existence of COVID-19 and later promoted its *Sputnik* vaccine, denying the effectiveness of Western vaccines – *"the usual stuff"* as a security expert summed up.

The pandemic also gave an opportunity for the populists of different stripes to seek visibility and influence, often employing the narratives echoing the Kremlin's propaganda during the parliamentary election campaign in autumn 2020. The abundance of political parties participating in these elections signalled the

[86] State Security Department of the Republic of Lithuania and Second Investigations Department under the Ministry of National Defence of the Republic of Lithuania, Grėsmių nacionaliniam saugumui vertinimas *[National Security Threats Assessment]* (Vilnius: Ministry of National Defence / State Security Department of Lithuania, 2020).

[87] UNCTAD Investment Policy Hub, "Lithuania. Law on the Protection of Objects."

tendency toward society's fragmentation, while individuals who want to take an active part in the political life of the country did not cooperate or consolidate their political activities.[88] *"During the Seimas elections in 2020, we observed the proliferation of minor political parties, which are supported by frustrated individuals. They are easy to target for the malign influence"*. On the other hand, no newly established political parties, except one after the split of a liberal party into two, made it to the Lithuanian parliament, Seimas.

Criticism was voiced regarding the content and quality of Lithuanian media in the ethnic minority languages Russian and Polish

The fact that the Lithuanian society is ethnically relatively homogeneous and the country does not encounter citizenship issues on the ethnic ground was repeatedly noted by respondents.[89] Nevertheless, respondents stressed the importance of a long-term integration and inclusion programme for ethnolinguistic groups as well as the new immigrants into the Lithuanian society: *"The long-term engagement with ethnic minorities as well as addressing the social exclusion and societies fragmentation should be addressed when the state institutions (including the Seimas) projects future development of the society and the state."*

The influx of political refugees from Belarus and Russia (at the time of these interviews) escaping political repression at home posed a major new challenge to the societal resilience in Lithuania. The respondents underlined that it is highly important to integrate them into society and thus to prevent them from being locked in their linguistic (usually Russian language) bubbles that might become a target for the malign information operations in the future. Lithuanian society cannot risk its cohesiveness and security: *"New immigrants keep living in their information bubbles, watch Russian TV and follow Russian media because of the language and cultural closeness, they are not integrated into the Lithuania society as they should be."* Nevertheless, in the opinion of respondents, the Lithuanian society is *"quite resistant to polarisation and extremism, however, the fragmentation of the society and rise of fringe parties and movements is an emerging risk."*

When talking about resilience-building among vulnerable groups, respondents noted that much more should be done to reach out to vulnerable groups. The society and, more importantly, the government should listen better to those groups, and the long-term comprehensive policies and programmes should be developed and implemented without delay. Civil society organisations (CSOs) are usually reliable partners designing policies addressing the issues that vulnerable groups face and should be better utilised in shielding those groups from foreign malignant influence activities. Otherwise, the vacuum created by inactivity or lack of attention from the government and Lithuanian CSOs is filled by GONGOs set up by Russia or China. Business representatives and security respondents particularly pointed out the growing role of Chinese GONGOs in Lithuania as an emerging risk in the information space when shaping public perceptions: *"China has become immediately visible when Lithuanian society organised support actions to Hong Kong and Taiwan."*

The fact that Russian-owned media outlets registered in Lithuania have a very small audience should not be underestimated. This media is used as a trigger to circulate pro-Kremlin narratives on social media groups, both open and closed. *"Russian media's tactics is to encapsulate itself with a small audience and increase media's visibility on social media. Moreover, Russian owned media registered in the EU reaches Lithuania not only in the Russian language."* As a recurrent risk, the respondents noted the impact of the Belarus state TV watched by the Lithuania population, including the ethnolinguistic population in the bordering areas with Belarus. In this regard, criticism was voiced regarding the content and quality of Lithuanian media in the ethnic minority

[88] Central Electoral Commission of the Republic of Lithuania, "Politinės kampanijos dalyviai [Participants of the political campaign]," last accessed 18 August 2022.

[89] At the beginning of 2020, Lithuanians accounted for 85.9% of the country's permanent population, Poles for 5.7%, Russians for 4.5% and others for 3.9%; citizens of the Republic of Lithuania accounted for 97.6% of the country's permanent population, 0.8% for Ukraine, 0.6% for Belarus, and 0.4% for Russia.

languages, Russian and Polish. Respondents named a few successful media projects but also indicated that there is a significant shortage of quality content and entertainment in national media in those minority languages allowing their speakers to feel more included into Lithuania's life.

Another risk voiced by the civic society, academia and business representatives was the absence of transparency of media ownership: *"Russia and China own and control the media directly and by intermediaries. The leading news portal Delfi (in Estonia, Latvia and Lithuania) is owned by offshore companies and thus the ownership is not transparent. TV3 Group is owned by Chinese funds and companies"*. Lithuanian respondents also discussed the urgency of improving the quality of reporting by both the national and regional media. *"Nobody monitors regional media whether and how disinformation cases are debunked or corrected."*

> *The institutional framework for building societal resilience in Lithuania is functioning and increasing its effectiveness, but respondents stressed the need for more agility and proactiveness*

Fact-checking is important, but it is not sufficient to build resilience to disinformation on its own. The interviewed Lithuanian respondents stated that the society is fragmented into the social bubbles which receive counter-disinformation very selectively. There are a number of communities that are not reached out to or do not want to be reached and stay in self-isolation. Thus, there is a paradox: *"While generally successful, efforts of strategic communications might be mostly preaching to the already converted."* Therefore, the respondents underlined the need for the impact assessment of activities to counter disinformation, noting also that social media poses the risk of fragmentation and even polarisation of the society: *"There are sufficient initiatives, but we do not know their effectiveness".* The Lithuanian Ministry of Culture occasionally assesses the mass media literacy of the Lithuanian population – the last assessment was conducted in 2017 and the new assessment was underway at the time the research interviews took place.[90] The survey focuses on the public's use of mass media patterns, communication skills and what the public thinks about mass media, thus providing a snapshot that might serve as an indicator of cumulative impact of those initiatives. However, a more systematic and frequent assessment is necessary.

Lithuanian respondents noted that in the age of social media and fast-spreading information, society is on the front line of confrontation and negative influences. They also debated the idea that even though it is effective, strategic communication alone is not sufficient for developing long-term social resilience and the ability of society to cope, adapt and quickly recover from critical situations or avoid further emergency escalation. In any case, policy, legal, organisational and other responses initiated by the government serve as an anchor for the rest of the society when coping with the acute and chronic stressors, including in dealing with malignant foreign influence and disinformation campaigns.

3.1.3. Responses

Information security as a part of national defence should be co-owned by a variety of players – state institutions, government agencies, local authorities, media organisations and the CSOs. Interviewed respondents agreed that the national legal framework for the information policy is in place and is functioning, but its effectiveness rests on the close cooperation and networking of all stakeholders of the information environment.[91] In addition, the legal procedure in countering the foreign-falsified content functions well within the national jurisdiction. *"Malign TV channels are banned, and they do not argue in court as they see that the legal structure is in place and is consistent and functioning"*. However, to be effective in setting the rules, accountability and transparency, it is essential to cooperate with

[90] Ministry of Culture of the Republic of Lithuania, *Žiniasklaidos priemonių naudojimo raštingumo lygio pokyčio tyrimas [Survey on Changes of Media Literacy Level]* (Vilnius: Ministry of Culture, 2021).

[91] Seimas, "Lietuvos Respublikos visuomenės informavimo įstatymas [Law on Public Information of the Republic of Lithuania]," *Valstybės* žinios, no. 71-1706, 26 July 1996.

social platforms on the international level, as media (especially social media) is *"a moving target."* Societal resilience is challenged by social media because, firstly, the social media giants such as Meta, Twitter and others are not subject to the Lithuanian legislation: *"it's up to them to decide to cooperate or not"*. Second, social media platforms and websites that are registered in third countries are subject to that country's jurisdiction. Third, the codes of conduct of social media are under development.

The institutional framework for building societal resilience in Lithuania is functioning and increasing its effectiveness, but respondents stressed the need for more agility and proactiveness. The Lithuanian Armed Forces were among the first to develop capabilities to monitor, assess and analyse the information environment in real-time. Today, all state institutions run fact-checking and strategic communication activities within the field of their competencies. For instance, the Ministry of Foreign Affairs has taken the lead in strategic communication to partner with state institutions to represent Lithuania's position abroad and to push the issue of information security to the top of the EU agenda. The State Security Department (VSD) and Second Investigation Department under the Ministry of National Defence promote public awareness of the national security issues by annually publishing a national threat assessment report and analysis on geopolitical trends.[92] The Bureau of Threat Prevention and Crisis Management Bureau (Group) in the Office of the Lithuanian Government steers and coordinates strategic communication activities between different state institutions, consolidating the comprehensive threat monitoring and crisis management mechanism. Lithuanian respondents highly regarded the performance of state personnel and volunteers in countering disinformation and propaganda, but also noted that the capabilities of state institutions differed depending on the institution: *"Civil servants should be trained on regular basis to understand and be able to counter disinformation and act efficiently to prevent and to cope with the cyber-info attacks"*.

Interviews with academia and NGOs representatives confirmed the need for a comprehensive and coordinated approach to media and information literacy (MIL) implementation at the national level. MIL knowledge and skills strengthen societal resilience. They pointed out that the design and implementation of the national media literacy policy mostly lie within the realm of three ministries – Ministry of Culture, Ministry of Education, Science and Sport and Ministry of National Defence. This indicates that a comprehensive national policy on media and information literacy is still under development. Lithuanian respondents noted that the MIL topicality was so far highly contextual depending on the political agenda at home and international politics. The interviewed respondents underscore the current pressing demand for MIL education for all groups of society.

Although the information about the intelligence work is not broadly known to the public, as noted by academia's and civil society's representatives, the Lithuanian respondents highly evaluated the national counterintelligence work and also highlighted the value of the cooperation with other Baltic states' intelligence agencies. Security respondents confirmed that the biggest intelligence threat to Lithuania comes from the Russian intelligence and security services which actively cooperate with their Belarusian counterparts. The system of free e-visas to Kaliningrad and St. Petersburg created favourable conditions for Russian intelligence services to gather information from incoming tourists and find suitable recruitment targets. Russian intelligence services tried to influence public life through the Russian compatriot community in Lithuania.[93] Chinese intelligence services look for targets in Lithuania in social networks: *"Cyber-enabled information operations against Lithuania happen very often"*. Business representatives welcomed the cooperation between the national intelligence and the Lithuanian business community in countering these threats.

Representatives of civil society, think-tank/academia and business clusters stressed the importance of the societal engagement: *"Public at large do not know how they could contribute to the work of media: whom to and when and how they could report about the noticed misconduct of media"*. The key issue is

[92] Ministry of National Defence of the Republic of Lithuania, *Grėsmių nacionaliniam saugumui vertinimas*.

[93] Ibidem.

a consistent build-up of the multidimensional structure for civil society to be involved in national security. Civic education, education on national security, on media and information literacy are crucial competences. In this regard, the Lithuanian National Education Strategy's efforts to clearly define the role of education as part of national security and include such topics as media and information literacy is noteworthy from a whole-of-society perspective.[94]

The key is a consistent build-up of the multidimensional structure for civil society to be involved in national security

Lithuania's civil society is directly engaged in the national information environment monitoring, fact checking and strengthening society's media and information literacy. A lot of work is undertaken by civic activists and volunteers working in IT, media, academia, education and business sectors. Civil society organisations in their fields of competence counter disinformation and are active in positive narrative communication. Although the state provides financial assistance to the civil society, the major financial support for the civil society comes from the international donors, which highlights the need address financial sustainability challenges, as the priorities and focus of those donors tend to shift and may not always reflect Lithuania's needs.

3.2. Latvia

3.2.1. Technology

The COVID-19 pandemic and the resulting shift to remote working arrangements in various sectors of the economy and societal life has underlined the importance of digital technology and cybersecurity to national resilience. Latvia has developed National Guards cyber units and has increased capabilities for mobilisation towards a whole-society approach, and the country ranked 25th in the world according to the International Cyber Security Index (NCSI) in 2021.[95] However, the risks for general society remain. Not only smartphones, but virtual assistants, routing devices and other smart technologies are raising concerns about mass data collection and low awareness of the population of what those entails. Those concerns are mostly related to the possible weaponisation of big data, collected through the data ecosystems of specific companies that provide hardware, software and services (including increasingly popular virtual assistants that can be used for harnessing data about the individual users).[96] The necessity for increased awareness and better knowledge in this area were highlighted by Latvia's Cyber Defence Strategy 2019-22.[97]

Concerns are mostly related to the possible weaponisation of big data, collected through the data ecosystems of specific companies that provide hardware, software and services

Another emerging issue was the increasing popularity of such search engines and recommendation platforms of Russian origin such as *Yandex, Rambler, etc*. Developing their own eco-systems (online and offline services), for example, of *Yandex*, only partly are looked at on the national level in Latvia. However, *Yandex.taxi* was mentioned by several respondents during the interviews. In October 2020, for the first time *Yandex* officially published the amount of data requests by the Russian security services.[98] As of Spring 2022, the mentioned services and platforms became

[94] Education is assigned an important mission in the field of national security - to develop the democratic culture of the country, to develop civil society, and to strengthen national security, see: Ministry on Education and Science of the Republic of Lithuania, *Valstybinė švietimo 2013–2022 metų strategija [National Education Strategy 2013-2022]* (Vilnius: Centre for Educational Supplies of the Ministry of Education and Science, 2014).

[95] e-Governance Academy, "National Cyber Security Index – Latvia," last accessed 18 August 2022.

[96] Jon Reisher, Charity Jacobs, and John Beasley, "Data as a Weapon: Psychological Operations in the Age of Irregular Information Threats," Modern War Institute, 5 February 2022.

[97] Artis Pabriks, *Informatīvais ziņojums "Latvijas kiberdrošības stratēģija 2019.–2022. gadam" [Informational report "Latvia's cyber security strategy 2019–2022]* (Riga: Ministry of Defence of the Republic of Latvia, 2019).

[98] "Transparency Report. Raskrytiye informatsii o zaprosakh [Trancparency Report. Request for disclosure of information]," Yandex, last accessed 18 August 2022.

banned in the Baltic states. Nevertheless, there are also other apps and data transmission and ownership tools that should be observed, and user awareness should be raised.

The popularity of streaming platforms has been increasing, especially during the pandemic. Piracy is still a problem in Latvian society, and many piracy platforms suggest entertaining media content in Russian for free while harnessing data about their users.[99] Forthcoming risks are also linked to one of the most popular streaming platforms – *Netflix*. In 2020, it announced close cooperation with the Russian National Media Group.[100] This group was mentioned in the report of the VDD, referring to Yury Kovalchuk, who is on the EU sanction list.[101] Predictably, the Russian interface of *Netflix* would be in high demand in Latvia because of the popularity of the Russian language. (In 2022, *Netflix* has suspended the work in Russia, which presumably involves cutting ties with the Russian partners as well).[102] As media consumption has become a round-the-clock activity and a diverse media diet includes different types of media, digital infrastructure plays a crucial role in monitoring disinformation and developing insights.[103] However, technological trends and user behaviours are increasingly posing challenges to those who seek to identify and understand disinformation activities. Monitoring by fact-checkers is problematic when it comes to platforms such as *Youtube*, *Viber*, *VK*, *Tiktok*, *OK*, *Whatsapp*, *Telegram*, where a lot of media content is shared through end-to-end encrypted messengers or in closed groups. As several respondents pointed out, monitoring of messengers is accepted for security services only. Paywalls also may become a challenge to collecting and analysing information: *"So far people have not got accustomed to pay for the content and the evaluation of the information environment discrepancy is not significant, but when paywall culture becomes more popular, the discrepancy will increase."* Given the new trend that media content should become more audial, it is also important to consider increasing audio monitoring facilities and capacities. It is also supported by media expert predictions known as the 'new golden age for audio.'[104] So far, according to additional interviews with media representatives, audio and audio-visual content is still more problematic to analyse in the context of detecting and countering disinformation.

Media in a broader definition – that now includes the streaming services, pirate torrents and illegal content platforms – are hardly traceable in traditional surveys

The Latvian respondents from think-tank/academia and government clusters pointed out difficulties in studying media consumption and trust in media because of the development of new platforms and eco-systems of information. Diversity of media diets of different audience groups is increasing. It includes the growing role of social media in news consumption. Media in a broader definition – that now includes the streaming services, pirate torrents and illegal content platforms – are hardly traceable in traditional surveys. While surveys are mainly focusing on Kremlin-related media channels (traditionally, TV channels), there are additional channels with the potential to be used for spreading disinformation.

China's broader interests in the technological domain were emphasised by several business representatives. When new technology start-up companies work hard to attract investment, sometimes they find themselves, in the words of one interviewed business cluster representative, as being "*taken care of*" by the Chinese investors. This becomes a choice between selecting a vector of growth linked

[99] Zane Brikmane, "Pētījumaa iniciatorus šokē intelektuālā īpašuma pirātisms Latvijā. Kā cīņā ar to sokas pašmāju autoriem? [The initiators of the study are shocked by intellectual property piracy in Latvia. How do local authors cope with this?]," *LSM (Latvian Public Broadcasting)*, 13 August 2020.

[100] Ilya Khrennikov, "Netflix Joins Putin Ally's National Media for Russia Rollout," *Bloomberg*, 2 September 2020.

[101] Latvian State Security Service, *Annual Report.*

[102] Mark Sweney, "Netflix subscribers in Russia launch class action for loss of service," *The Guardian*, 13 April 2022.

[103] Deloitte Center for Technology, Media and Telecommunications, *Digital media trends survey, 14th edition. COVID-19 accelerates subscriptions and cancellations as consumers search for value* (Deloitte Development LLC, 2020).

[104] Nic Newman, *Journalism, Media, and Technology Trends and Predictions 2020* (Reuters Institute / University of Oxford, 2020).

with Europe that often comes with difficulties in obtaining financing or with China that is ready to provide funding but evokes significant national security concerns. For the European investors, considerations such as grant sustainability are highly relevant. Increased technological dependence on China in everyday activities of consumer, business and state administrations was one of the emerging risks that the interviewed respondents referred to, while think-tank and academia representatives pointed out close Chinese and Russian intelligence cooperation as a high-level risk when it comes to such dependence.

> *The use of entertainment in spreading disinformation has been flagged as a newly recognised risk vector*

3.2.2. Society, Politics and Media

A few respondents pointed out that the COVID-19 situation during 2020-21 could result in an economic downturn, which would be used to strengthen the 'failed state' narrative advanced by Russia. Academia related respondents mentioned the need to follow how the pro-Russia propaganda point that *"we should develop a better connection with Russia"* would continue evolving in the public space.[105]

Another important issue to follow is the securitisation and weaponisation of history in and by Russia that moved into an active phase and targeted Latvia as an alleged *"revisionist of history."* It contains many well-known elements that were mentioned by the respondents, such as the so-called *bessmertnyj polk* ("The immortal regiment"), protection of the Soviet army monuments, the use of St. George's ribbon, etc.[106] As one interviewee noted, *"the 9th May is the only (event), which is able to collect so many people at one place, so the Kremlin continues to exploit it."* However, history-tuned public diplomacy as a supportive element of the currently developing eco-system for *"defending the truth"* is a fairly new aspect of Russia's approach. At the same time, Latvian government authorities quickly adapted to this trend and developed both symmetric and asymmetric responses.

The use of entertainment in spreading disinformation has been flagged as a newly recognised risk vector. The narratives are not new but, according to some interviewed respondents, Russia intensified investments in history-related entertainment. Russian-funded movies are shown in Latvian theatres and books are widely distributed in local bookshops, etc. While the general evaluation of Russian cultural events in Latvia is assessed as decreasing, one respondent underlined the activities of Russian artists in Latvian regions. These activities remain unnoticed in the capital, yet they are able to attract Russian-speaking users not only from smaller towns, but also from other countries (referring to an Estonian numberplate at a parking lot in Valmiera, a city in the northern part of Latvia where a concert of a Russian stand-up comedian took place). Some civic activists mentioned that cultural events in the Russian language are needed for Latvian society and the desire of the audience to see specific Russia-related celebrities should be satisfied. At the same time, their narratives and the activities of celebrities should be monitored.

Academia representatives referred to a significant increase in the sense of a threat of Russian language use in Latvia by the Russian-speaking communities. As a potential risk, the researcher connected it with the decrease of popularity of a political party, Harmony, that represented their interests. Some defence and security related respondents in Latvia noted that thanks to successful activities of the Latvian security services, some traditional pro-Kremlin actors (agents of influence) significantly reduced their political activities (visibility of activities reduced). Interviewed respondents do not connect it with less financial flows from Russia, but to possible changes of tactics by Russia. Possible activities of strengthening anti-institutional voices are based on political and ideological parallelism. General

[105] In the pre-Covid survey, good relations with Russia on the level of public perception: 32% strongly agree and 50% somewhat agree, that Latvia's interest are best served by maintaining strong relations with Latvia. It is less that overall support to the EU. According to the same survey relations with the US and China are less important, see: International Republican Institute, Center for Insights in Survey Research, "Public Opinion Poll: Latvia, January 10 - February 2, 2020," last accessed 18 August 2022.

[106] "Bessmertnyj Polk Riga [Immortal Regiment Riga]," Bessmertnyj Polk Riga, last accessed 18 August 2022; "Rubrika "Vojna s pamyatnikami" [Rubric "War on Monuments"]," Baltnews.lv.

extreme pessimism about Latvia's *"viability and performance"* was also mentioned in Mārtiņš Kaprāns and Inta Mieriņa's research on ideological polarisation.[107] One academia-related respondent pointed out the importance of social exclusion, referring to the urban-countryside gap and openness to populism within specific groups, while not very present through geopolitical issues. Another risk connected to political culture was identified by a civic opinion leader who pointed out that conservative parts of the Latvian language audience have the potential to be influenced by Putin's narratives on traditional values, as well as on increasing the gap between Europe and the United States.

Democracies are stronger when civil society joins forces with the government in protecting the society against disinformation

The majority of the interviewed respondents mentioned that the activity of Russian influence agents and GONGOs was perceived as decreasing. At the same time, China has increased its activities. Several respondents highlighted China's activities particularly in relation to the Latvian academic and research institutions (activity of centres, conferences, joint projects).

3.2.3. Responses and Related Issues

The State Defence Concept, adopted in September 2020, refers to the wide scope of hybrid threats, which includes psychological resilience as a part of national defence.[108] The main challenge of an institutional response lies in the necessity to act according to the values of a liberal democracy. Information activities of authoritarian foreign actors are exploiting vulnerabilities of democracy. There is a general understanding that implemented regulation should not harm basic democratic values, including civic freedoms (as freedom of expression and freedom in private life). At the same time, democracies are stronger when civil society joins forces with the government in protecting the society against disinformation. Latvian respondents mentioned numerous initiatives by the civil society, media, think-tanks and academia to increase awareness: "*I really see that it works, all these grants and events reading qualitative analysis on (entertaining media), for the specific audience*".

Some representatives of the think-tank/academia and media clusters, however, pointed out negative effects when media literacy-oriented grants are provided to the media outlets that are not creating quality content or, in parallel, are creating misleading content. To increase the quality of winning projects, one of the think-tank/academia cluster representatives called for increased responsibility of the selection committees. Frequently, they are not paid for this type of job and are potentially not motivated to invest time to study the question in-depth.

Trivialisation of the cognitive processes could be harmful for debunkers themselves, as they become a tool of amplification of disinformation

While there is a growing number of disinformation tracking and elimination initiatives in the media, the risks of amplification of disinformation, or inappropriate fact-checking are also increasing, as highlighted by one expert working with civic initiatives as well as debunking.[109] A representative of one of the think-tanks in Latvia shared concern that inexperienced researchers are inclined to use the easiest way of checking resources of Kremlin propaganda and therefore might unknowingly contribute to spreading some false narratives. Among the main problems is the lack of understanding of effectiveness of both disinformation campaigns and debunking products. Trivialisation of the

[107] Mārtiņš Kaprāns and Inta Mieriņa, *Ideological Polarization in Baltic Societies. A Cross-National Survey Report* (Riga: University of Latvia, 2019), 76.

[108] Saeima, "Par Valsts aizsardzības koncepcijas apstiprināšanu [National Defence Concept]," Likumi.lv (Legal Acts of the Republic of Latvia), 24 September 2020.

[109] Whitney Phillips, *The Oxygen of Amplification, Better Practices for Reporting on Extremists, Antagonists, and Manipulators Online* (Data & Society Research Institute, 2018).

cognitive processes could be harmful for debunkers themselves, as they become a tool of amplification of disinformation by bringing marginal topics and highlighting them for their audiences (priming and repeating).

Yet, the awareness of harmful or toxic fact-checking is growing. One of the media sector respondents mentions the need for a local fact-checking service in order for journalists to be able to outsource fact-checking for their media projects. The informational environment would benefit from more elaborate requirements of this notion in grant projects.

New challenges may increase dissatisfaction in society and create a breeding ground for the spread of disinformation

Another challenge to an effective response to disinformation pointed out by media representatives, think-tank activists and civic opinion respondents is online attacks on debunkers. *Re:Baltica* – an investigative journalism centre – took initiative to build a fast response line with the police.[110] Psychological pressure is often exerted against fact-checkers (including online harassment), and there is a need to strengthen the journalistic community.

The question of definitions (what is and what is not disinformation, misinformation, etc), as well as professional standards were pointed out by the majority of respondents. It also raises a question of how to regulate bloggers and social media actors, who pretend to be accredited as media but do not follow media standards and regulations: "*Everyone pretends to be a journalist*". The environment has changed significantly: "*Not all media are in associations*," and the above-mentioned media are not registered as media at all. "*Anyone can say that they are a journalist, as it is not well-regulated, and thus can ask for accreditation as media, even they just write blogs. Normative regulation is not in order.*"

The number of media literacy projects is growing. Compared to the media literacy audit of 2016, many new actors were mentioned and positively assessed by the respondents. However, according to interviewees, there is still space and a need for developing projects to enhance the resilience of vulnerable groups. In designing such projects, the negative effects of media literacy campaigns on some vulnerable audiences – such as accusations against the fact-checkers in censorship and biased selection of topics and facts – should be taken into account. The question of language of these activities also arises. For instance, activities related to the COVID-19 response led to increased information dissemination in the Russian language.[111] The respondents also pointed out problems with measuring the effectiveness of media literacy projects.

Concerns are mostly related to the possible weaponisation of big data, collected through the data ecosystems of specific companies that provide hardware, software and services

In disinformation-related research, some respondents pointed out the need for detailed analysis of audiences, including Latvian linguistic audiences in rural areas and small towns and younger generations, as well as continuing research on the Latvian diaspora abroad.

3.3. Estonia

3.3.1. Economy and Technology

Even if the majority of the interviewed respondents did not rate Estonia's economic dependence on Russia and China generally high, money laundering, the COVID-19 pandemic related pressure on the tourism sector and a hasty transition to renewable energy are perceived as threats that could leave hundreds of people unemployed. Therefore these factors

[110] Sanita Jemberga, "Dārgā policija, sveicieni no (vēl dzīvas) stervas [Dear police, greetings from a (still alive) bitch]," *Delfi*, 17 December 2020.

[111] Artis Pabriks, "Zdravstvuyte, uvazhayemyye zhiteli Latvii! [Dear residents of Latvia!]," Ministry of Defence of the Republic of Latvia, last accessed 18 August 2022.

were seen as the new challenges which may increase dissatisfaction in society and, in turn, create a breeding ground for the spread of disinformation. Russia and China were still considered to be the main protagonists in this field.

In the shadow of the image building campaign, China's influence is expanded through government subsidised takeovers of large companies. For example, the *Nordic Cinema Group* and, once the Estonian company of the year laureate, aircraft maintenance and repair services provider *Magnetic MRO*, have been acquired by Chinese companies.[112] There has also been an attempt to solely finance and build a new LNG terminal in Paldiski by one of the Chinese construction companies.[113]

> *China's strategy in Estonia was more difficult to notice because activities seemed to be designed to gain influence over a longer period of time while avoiding direct confrontation or conflict*

When it comes to vulnerability to digital warfare, the study showed that the popularity of foreign social media platforms was ranked high by a vast majority of the Estonian respondents as most popular platforms are all of foreign origin. The main challenge in this regard was considered to be the limited options to regulate the content because foreign social media platforms are located outside of the state legislation. Additionally, a certain degree of dependence on Chinese technology was noted. However this dependence was not considered Estonia-specific, but rather a part of the wider western dependence on Chinese mass production. Technological dependence on Russia was rated as minimal, although there is a presence of Chinese technology through *Huawei* products and certain Russian presence through social media platforms and apps like *Yandex* and *VK*.

3.3.2. Society, Politics and Media

Russia's activities were characterised by a constant flow of information that supports social instability. However, the dissemination of disinformation has become more strategic, and instead of supporting specific influencing agents or organisations, instability in Estonia is sought by a strategically placed agenda, enriched with disinformation and a combination of sources – traditional media, social media, ROC and the entertainment industry, – in order to create gaps both along the lines of political ideology and ethnic origin in the Estonian society.

Although no major dependencies were noted, and the impact of China's activities has been small in the past due to the lack of direct contacts, respondents said that the recent activation had become noticeable and, unlike Russia, China's strategy in Estonia was more difficult to notice because activities seemed to be designed to gain influence over a longer period of time while avoiding direct confrontation or conflict. The methodology used was wide-ranging propaganda, employing various lobbyists and advertising companies, as well as opinion articles together with fancy receptions and media events, to create a positive image in general. According to the vast majority of the respondents, however, the activities of both Russian and Chinese GONGOs or direct influence agents were not very visible in the public information space of Estonia.

> *Although the ethnic gap in Estonian society is said to be slowly narrowing, successful integration has not yet been achieved*

According to the majority of the respondents interviewed, political movements in Estonia were not considered to be directly related to

[112] Lennart Kruuda, "Eesti aasta ettevõte müüdi 40 miljoni euroga hiinlastele [Estonian Company of the year sold to Chinese for 40 million euros]," *Postimees*, 3 January 2018; Urmo Andressoo and Mait Kraun, "Hiinlased ostsid Eesti suurima kinoäri [The Chinese bought the largest cinema company in Estonia]," Äripäev, 23 January 2017.

[113] European Parliament, "Välismaine ettevõtete ülevõtmine Covid-19 kriisi ajal: saadikud nõuavad võrdseid võimalusi [Foreign takeovers in Covid-19 crisis: MEPs push for level-playing field]," 24 June 2020.

the Kremlin or CCP. However, many interviewed respondents said that there has been an increase in polarisation and radicalisation noted in Estonia between the conservative and liberal axis which hostile foreign countries could make use of. Although the ethnic gap in Estonian society is said to be slowly narrowing, successful integration has not yet been achieved. A noteworthy issue highlighted by some Estonian respondents was that, amongst the young people from the linguistic and/or ethnic minority – and even amongst the ones who have learned Estonian – a feeling of exclusion can still be identified in some regards. Therefore, inclusion of young people from minority backgrounds needs more attention and continuous tailored work.

The lack of a longer-term strategy is a new challenge in the entire field of information security, and strategy on how to approach China should have the priority

Concerning the media, the majority of Estonian respondents rated the general impact of foreign media that disseminates disinformation in Estonia as medium or rather small. Russian and Chinese channels known to disseminate disinformation have gained little ground in Estonia. Their trust ratings are low compared to the local channels that surpass them in both popularity and trust, amongst both the Estonian and Russian-speaking populations.[114] Nevertheless, the Russian state media still had a considerable audience amongst the Russian-speaking minority as of 2020-21. The interviewed respondents noted the political bias of certain local newspapers and increasing spread of false information presented in the so-called alternative media as emerging threats. The latter problem is especially amplified by the public's, including youth, lack of critical thinking and lack of consciousness when consuming information, while the ideological affiliations or sympathies of some major media outlets have emerged as new problems. In the light of these problems, a growing loss of trust in the media in general has also been noted. Here, the interviews showed that the older generation and the linguistic minority were assessed to be the most vulnerable.

3.3.3. Responses

When it comes to institutional development, the majority of the Estonian respondents rated the institutional development of information security as 'very good' or 'good', and the majority of respondents also assessed the quality of research conducted in this field as 'good'. However, according to the interviewed respondents, there is a need for longer-term research in the field of disinformation. The Estonian respondents noted that the countermeasures should be better informed and coordinated, because many interviewed respondents consider the current research to be too project-based, while the scope is too broad and not sufficient to address the vulnerable target groups. It became therefore evident that the lack of a longer-term strategy is a new challenge in the entire field of information security, and strategy on how to approach China should have the priority in the action plan because less is known regarding their influence activities.

Focusing on countermeasures, Estonia ranked third in the world according to the National Cyber Security Index in 2021.[115] According to officials related to the field, DDoS and ransomware attacks are a constant phenomenon, although no major breakthroughs have been achieved by the attackers. The interviewed respondents noted that Estonian cybersecurity is based on effective cooperation between the state and the private sector, as well as international cooperation with allies. "*We, in Estonia, do not have the capacity to be top performers, but our strength is a uniform level and the ability to quickly apply modern capabilities in practice.*" For instance, in an emergency situation caused by the COVID-19 pandemic, RIA has also made the internationally recognised set of cyber security measures "CIS 20 Controls" available in Estonian that can be used by small, medium and large size companies to ensure the security of

[114] Kantar Emor, "Eesti elanikud usaldavad enim ETVd ja ERRi uudisportaali [ETV and ERR are the most trusted media channels among residents of Estonia]," Press Release, 30 March 2020.

[115] e-Governance Academy, "National Cyber Security Index – Estonia," last accessed 18 August 2022.

their systems.[116] The same authority, together with Telia, one of the main internet and communication service providers in Estonia, created a cyber security hotline aimed at one of the most vulnerable parts of the population – the Russian-speaking seniors.[117] However, according to the interviewed respondents, cybersecurity needs to be continuously developed.

According to the interviewed respondents, different cyber-attacks are common. However, Estonia's strength is also seen in its conscious action in the field of trade and technology that has helped to avoid direct dependence on Russia and China and therefore also the worst-case scenarios. In the case of the IT sector, Estonia has been able to turn the disruptive attempts into an opportunity by becoming a leading promoter of digitalisation and cybersecurity in the EU.[118] Estonian respondents assessed dependence on China and Russia in the field of cybersecurity and digital technology as low because all Estonian state systems are built to European or US hardware and cryptographic standards. Furthermore, in March 2020, the Estonian Parliament, Riigikogu, also approved an amendment to the Electronic Communication Act according to which the usage of certain types of technology may be denied from being used in strategic communications networks if the product or its manufacturer is not considered "trustworthy and safe."[119] This further reduces possibilities for the technological penetration of the information and cyber space of Estonia by the hostile foreign powers.

There is a need for systematic analysis of the public information space based on big data and AI-enabled tools to stop disinformation at an early stage

In countering disinformation, the efforts include major media outlets creating their own fact checks, participating in the international debunk.eu project (e.g. *Delfi* news portal) and creating a separate page focusing on raising awareness on media consumption (e.g. ERR).[120] The majority of the respondents did not identify serious cases of the Estonian media channels consciously broadcasting disinformation in their channels and deemed the self-regulation of the Estonian media sufficient. Nevertheless, in today's rapidly changing information society, the new challenge is to avoid the spread of disinformation caused by the poor choice of primary sources, reckless transposition of narratives and insufficient fact-checking, which can inadvertently help the spread of false information. Also, since the ability to monitor information flows based on big data is restricted for the public and for most institutions due to the limited access to such technology, there is a need for a technological solution that would allow the systematic analysis of the public information space based on big data and using Artificial Intelligence (AI)-enabled tools. Such wish was expressed by many interviewed respondents as it would help to identify, detect and thereafter stop the spread of disinformation at an early stage by making malicious attempts public before they gain ground.

There was also an acknowledgement of some societal groups in Estonia being informationally more vulnerable than the others.[121] In this regard, the role played by the civil society is of utmost importance. Every second interviewee rated Estonian civil society's performance in countering disinformation as 'good' or 'rather good', and no one rated it with the worst score. However, weaknesses include the over-reliance of civil society on state funding, limited reach and low activity among the Russian-speaking population.

[116] Information System Authority of the Republic of Estonia, "RIA juhend ja videod aitavad ettevõtteil ennast küberruumis kaitsta [RIA's handbook and videos help companies protect themselves in cyberspace]," 8 April 2020.

[117] Information System Authority of the Republic of Estonia, "Eakad saavad aasta lõpuni küberturvalisuse nõu infoliinilt [Until the end of this year, senior citizens can call the helpline for advice on cybersecurity]," 16 November 2020.

[118] Josh Gold, "Estonia as an international cybersecurity leader," E-Estonia, 21 August 2019.

[119] Riigikogu, "Elektroonilise side seaduse muutmise seadus 138 SE [Electronic Communications Act Amendment Act 138 SE]," *Riigi Teataja*, RT I, 33 (2020).

[120] "About Debunk EU," Debunk EU, last accessed 18 August 2022; "Sari "Faktikontroll" [Serie "Fact Check"]," Delfi, last accessed 18 August 2022; "ERRi meediapädevuse projekt "Meediataip" [ERR's media literacy project "Meediataip"]," ERR, last accessed 18 August 2022; "Faktikontroll "Õige või vale" [Fact Check "True or Wrong"]," Postimees, last accessed 18 August 2022.

[121] Alona Shestopalova, "Forgotten and Potentially Vulnerable: Why the Online Activity of Middle-Aged Women Matters During Global Information Warfare," ICDS Policy Paper, April 2022; Teperik, "Democracy, 'Alternative Reality'."

As for the legal framework, most respondents considered it to work well in Estonia. However, they also pointed to shortcomings in detecting, preventing and stopping the spread of disinformation, especially in the digital world, where many interviewed respondents consider it necessary to improve law enforcement: *"Estonia, like the EU, focuses more on the protection of the individual but could broaden its perspective by addressing the impact of disinformation in general by changing the procedures and improving the speed of response".* While international cooperation is useful, and even essential, for social media and digital technology regulation to prevent their exploitation for disinformation campaigns, agreement at the international level should always be discussed first at the national level with all parties in order to avoid a situation such as with the EU Regulation 910/2014 that set universal standards for digital ID services but lowered the already achieved level of encryption in Estonia.[122]

> *In 2021, the Lithuanian respondents were not very optimistic about the effectiveness of the national legal framework to counter information threats*

3.4. Impact of Turbulent Developments in 2021

The year of 2021 was characterised by several overlapping crises, including implications of the situation in Belarus, the COVID-19 pandemic, perturbations in domestic politics and arising socio-economic problems. Combined effects of all factors created a fertile ground for disinformation campaigns in the Baltics. Given the context, autocratic Russia and China have tried to benefit from the complex situation not just globally but also regionally and locally.[123]

The Kremlin continued projecting its strategic narratives against the Baltic states.[124] In addition to the COVID-19-related topics, the situation with the migration crisis was also used in propaganda.[125]

As noted by many interviewees, some parts of the population in the Baltic states were informationally influenced by disinformation campaigns based on conspiracy theories. Thus, 27% of Latvians, 27% of Lithuanians and 16% of Estonians confirmed to believe in some of the COVID-19 pandemic conspiracy narratives in 2021.[126] To re-examine the perceptions about resilience in the Baltics, the same representatives from five clusters were surveyed again, a year after the first round of the interviews and surveys. Gathered answers provided insights into the situation of whether society in each country learned and implemented some lessons from these crises and how the cross-sectoral cooperation (including communication and support) should be improved. Special attention was also paid to the role of media and information consumption by the public. As of autumn 2021, 63% of Estonians, 43% of Lithuanians and 42% of Latvians confirmed that they relied on the work of professional journalists in times of societal crisis.[127]

3.4.1. Lithuania

The respondents, interviewed and surveyed in Lithuania in 2021, noted that the popularity of Russia and/or Chinese controlled media has increased, compared with the previous year. In their opinion, there were a remarkable number of various vulnerable groups within Lithuanian society who were influenced by the Russian and/or Chinese propaganda.

The interviewees expressed the opinion that the degree of societal polarisation and radicalisation that can be potentially exploited by and/for the Russian or/and Chinese interests has increased since 2020, as the domestic situation became more complex.

[122] European Parliament and the Council of the European Union, "Regulation (EU) No. 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC," *Official Journal of the European Union* L 257/73 (28 August 2014).

[123] Edward Lucas et al., *Post-Mortem: Russian and Chinese COVID-19 Information Operations* (Washington DC: Center for European Policy Analysis, 2021).

[124] Holger Mölder and Vladimir Sazonov, "The Kremlin's strategic narratives on the Baltic states during the COVID-19 crisis," *Kwartalnik Bellona* 70, no. 4 (2020): 1–10.

[125] "Lithuanian armed forces analysts: disinformation has expanded, especially about the migration crisis," *Baltic News Network*, 15 December 2021.

[126] Hajdu, Klingová, Milo and Sawiris, *GLOBSEC Trends 2021.*

[127] Jõesaar, Rožukalne and Jastramskis, "The role of media in the Baltics."

In 2021, the Lithuanian respondents were not very optimistic about the effectiveness of the national legal framework to counter information threats and assessed it lower than in the previous year. Many respondents highlighted the significant decrease in the countermeasures to disinformation as introduced by the country's civil-society organisations, although the regularity and quality of disinformation and resilience-related trainings to vulnerable groups was assessed slightly better than in 2020.

> *The respondents highlighted that Latvian society has rather not learned and implemented the lessons from the COVID-19 pandemic*

According to the interviewees, the societal preparedness for rapid mobilisation during the multifaceted crisis in Lithuania can be assessed as 'intermediary', so there are some important lessons to be learned from the pandemic crisis management.

3.4.2. Latvia

The perception of how many vulnerable targeted groups are influenced by the Russian or/and Chinese governments has changed, compared to 2020. The majority of the interviewed respondents marked 'remarkable' for the amount of such groups in 2021, while the most common answer in 2020 was just 'several.' There was also a slight increase in assessing the degree of societal polarisation and radicalisation that can be potentially exploited by/for Russian or/and Chinese interests. Two thirds of respondents in 2021 evaluated it as 'high' or 'very high,' while in 2020, the majority evaluated the degree as 'intermediate' or 'low.'

Perception of the level of institutional development in the sphere of information security of Latvia decreased from 2020 to 2021. If in 2020 most of the respondents evaluated it as 'high' or 'very high,' then in 2021, the most common answer was 'intermediate' and 'low.'

The same as for 2020, in 2021 there is a discord in the perception of the level of comprehensiveness of the legal framework as it regards detection, prevention and disruption of information threats and vulnerabilities.

While estimating the effectiveness of countermeasures to disinformation and propaganda introduced by the country's CSOs and initiatives, the perception of the Latvian pre-selected respondents has changed from 'highly effective,' 'effective' and 'somewhat effective' in 2020 to mostly 'rather ineffective' in 2021. There is still a significant diversity of assessment of regularity and quality of counter-disinformation and resilience-related events conducted for vulnerable groups. In both 2020 and 2021, the most common answer is 'rather poor.'

As to the question of the level of societal preparedness in relation to the rapid mobilisation during an ongoing multifaceted crisis, most of the Latvian respondents who agreed to fill in the survey in 2021 evaluated it as 'low' or 'very low.' Moreover, the respondents highlighted that Latvian society has rather not learned and implemented the lessons from the COVID-19 pandemic.

3.4.3. Estonia

In 2021, the Estonian non-governmental representatives estimated the impact of Russian and/or Chinese media channels to be 'rather high', while the state-affiliated representatives assessed it to be 'low'. The number of vulnerable groups influenced by these channels, however, is considered 'high' by majority of the interviewed respondents both in 2020 and 2021.

> *Compared to 2020, the discord has increasingly switched from ethnic and language-based views to the liberal vs conservative axis*

Many interviewees noted that the polarisation of the society is even more relevant after the COVID-19 crisis. Noticeably, however, compared to 2020, the discord has increasingly switched from ethnic and language-based views to the liberal vs conservative axis.

The regularity and quality of counter-disinformation and resilience-related events conducted in Estonia for vulnerable groups remained a persistent challenge. Nevertheless, the estimation regarding effectiveness of countermeasures to disinformation and propaganda as introduced by the country's civil society organisations and initiatives were assessed by the Estonian respondents positively, as they rated the COVID-19 countermeasures as 'somewhat effective'.

One of the major challenges is low societal preparedness to handle multi-layered information crises that require more coordination and cooperation between various stakeholders

Despite the pandemic crisis, the surveyed respondents also marked some positive changes in the level of institutional development and comprehensiveness of the legal framework in terms of detection, prevention and disruption of information threats and vulnerabilities.

4. Major Sectoral Similarities and Differences in the Baltics

Based on the combined results from in-depth interviews and the survey questionnaire, there is a significant difference between governmental sector officials and respondents from other sectors in assessing the visibility and effectiveness of protecting vulnerable target groups, with the former considering the situation to be significantly better than the rest. This indicates that the activities of the area specific institutions have gone largely unnoticed and should be perhaps better highlighted to the public.

However, the majority of respondents in Estonia, Latvia and Lithuania were united by the opinion that China's influence has remained hidden from the sight of the Baltic societies, which indicates the need for better strategy towards countering China's influence. At the same time, many interviewed respondents addressed the exposure of ethnic or linguistic minorities to malignant campaigns which is caused by the relatively large role of the traditional and/ social Russian media amongst the Russian (or Polish)-speaking population and a presence of coping difficulties caused by different factors, making them more vulnerable to disinformation.

The general number of highlighted strengths and opportunities by the academics is noticeably lower than those of respondents representing other sectors. It might indicate a certain lack of systematic applied research done in the field of resilience to disinformation in the Baltics. However, the day-to-day practical contact that business and civil society representatives maintain has clearly become evident through their contribution, confirming the need for cooperation between the state authorities, civil society, academia and private sector. While assessing new challenges related to disinformation, state officials have pointed out significantly fewer new challenges than interviewed respondents from the business sector. It leads to the conclusion of insufficient communication between public and private sectors in the Baltics, as the quality of systematic responses was assessed with a high variation among business representatives and government officials.

Vulnerability to the digital threats was considered the weakest point by academics, independent experts and government officials, but not so by the media and business sector representatives. The latter concentrated more on technological dependence, while others focused more on the role of foreign-controlled social media and the limited legal capacity to regulate their content on a national level. One of the major challenges that remains is low societal preparedness to handle multi-layered information crises that require more coordination and cooperation between various stakeholders. In fact, some sectors (e.g., business community, media, academia) do not perceive themselves naturally as part of crisis management. Moreover, there is no universal understanding of resilience among different sectors as their threat perceptions diverge on a larger scale. Building awareness through constant dialogue is an important prerequisite for elaborating common denominators of resilience in various sectors. The state should take a leading role in this process as overconfidence about its own capacity for information crisis management (and underestimating those of non-state actors) might create a serious threat to national security.

> *As important background for resilience, the general strength of the Baltics arises from the historical memory and consciousness*

Conclusions and recommendations

Although the study encountered several challenges in assessing and weighing the perceptions about the state of resilience to disinformation in the Baltic states, it still managed to address different angles of the complex socio-political situation during 2020-21. The analysed data, combined with experts' observations, provided the authors with a good opportunity to draw some conclusions and recommendations the relevance of which remains high, especially in the light of Russia's aggression against Ukraine and its implications for the Baltic states.

As important background for resilience, the general strength of the Baltics arises from the historical memory and consciousness that help to recognise the malicious methods and influence tactics used by foreign actors (especially Russia), learn from them and develop countermeasures, making the societies more resilient to the spread of disinformation and influence campaigns of adversaries. Chinese influence in the Baltic states is recognised as rather minor, with no worrisome effects on the population. The most popular media channels in the Baltics are largely neutral towards China, but there is a rising awareness within the Baltics of the various threats posed by China.

The views of the sanctions on Russia since spring 2022 – an economic factor of malign influence – is considered to play a marginal role on foreign disinformation against the Baltic states, as dependency on Russia is being minimised in all possible areas, and dependency on China is being mitigated through the EU and relations with the United States. Western-focused internationalisation of all spheres in the Baltics has proven to have a long-term positive impact on developing national resilience against foreign-led disinformation. Nevertheless, some domestic political actors target pro-Western vectors of development through their rhetoric and populist campaigns of disinformation. If this trend continues, the political establishment in the Baltics should be aware of the severity of possible consequences to societal resilience and national security.

> *Dependency on Russia is being minimised in all possible areas, and dependency on China is being mitigated*

Resilience to disinformation is one of the contributing factors to strengthening electoral integrity and thus ensuring the continuation of democratic traditions.[128] Such understanding emphasises best practices in developing and promoting tools for transparency and digital resilience of vulnerable groups in politics.[129] Moreover, it promotes youth education based on dialogue and democratic skills to eliminate structural inequalities and to make societies more inclusive.[130] There also should be an ensured continuation of support programmes

[128] Beata Martin-Rozumiłowicz and Rasto Kužel, *Social Media, Disinformation and Electoral Integrity* (Arlington, VA: International Foundation for Electoral Systems, 2019).

[129] Kristina Wilfore, *A Digital Resilience Toolkit for Women In Politics Persisting and Fighting Back Against Misogyny and Digital Platforms' Failures* (#ShePersisted, 2022).

[130] Markus Pausch et al., *Resilience Against Anti-Democratic Tendencies through Education. Competences for Democratic Culture in European Social and Youth Work* (Salzburg/Strasbourg/Toulouse/Vienna/Warsaw: Council of Europe, 2021).

focused on publishing educational materials on disinformation threats for younger generations of Baltic citizens.[131]

The importance of a systematic response, cross-institutional coverage and information security are considered by most of the respondents to be among priorities in the Baltics, as state institutions have achieved some success in hampering the spread of foreign unfriendly GONGOs and narrow the long-standing ethnic divide, especially amongst younger generations. Since new waves of migration can still challenge the social cohesion in the Baltic states, this topic should be closely monitored not just by respective authorities but also by media and civil society organisations to raise awareness among the population about foreign-led or domestic attempts to amplify migration-related disinformation, maximise a divisive effect of the issue and enhance societal polarisation.

> *Local media contribute to coherent whole-of-nation conversation and reduce harmful effects of disinformation, thus bridging the ethno-linguistic or even generational gaps*

National resilience to disinformation can be maintained and further increased by the development of national and local quality-media. Broadcasting content created by professional journalists in both national languages and Russian (or Polish), local media contribute to coherent whole-of-nation conversation and reduce harmful effects of disinformation, thus involving and gradually gaining the trust of Russian (or Polish)-speaking part of the population in the Baltics and bridging the ethno-linguistic or even generational gaps. Measures for strengthening and empowering national or local public service media should address:

- developing good practices for sustainable media financing, including hyper-local media;
- revising the role of journalistic community and increasing their practical skills of cognitive resilience;
- enhancing cross-sectoral networking and developing information and digital literacy related infrastructure amid the growing challenges for hybridisation of newsrooms;
- spreading awareness of the issues of mental health and the well-being of the journalist community.

Generalised and uncritical securitisation of the problems and vulnerabilities of the ethno-linguistic minorities in the Baltics was readily acknowledged by many respondents as a serious problem in itself, therefore more tailored methods of strengthening social cohesion should be developed and implemented by responsible authorities in cooperation with relevant stakeholders. As there is more evidence regarding non-ethnicity related fragmentation in the Baltic societies, stigmatisation of a language or ethnic background is counterproductive as it can also be used in disinformation campaigns.

Since every serious crisis tends to challenge various aspects of nation's resilience, the information domain remains ever-evolving as proved by the lessons learned (or not learned) from the COVID-19 pandemic, weaponised migration or any other societal crisis further magnified by domestic populist politics. Therefore, resilience to disinformation in the Baltics requires state agencies, media houses, CSOs and socially responsible businesses to have access to modern tools, with the capacity for monitoring media and social networks to enable detection and prevention of the spread of disinformation at an early stage. A holistic approach and interconnectedness of various stakeholders ensures the cross-fertilisation of effective measures and cross-functional utilisation of resources (including competent workforce) to form a collective cognitive immune system of a society.

[131] Several good examples in various languages can be referred as: Solvita Denisa-Liepniece, *Sazvērestības teorija [Conspiracy theory]* (Riga: Latvijas Mediji, 2022); Dmitri Teperik, *Kak zhiteli Elu svoj volshebnyj les ot nepravdy zashchishchali [How the inhabitants of Elu protected their magic forest from lies]* (Tallinn: MTÜ Ida-Viru Noorteakadeemia, 2021); Solvita Denisa-Liepniece, *Zubami "Shchelk" ili Volk manipulyator* (Chișinău: Vidzeme University of Applied Sciences, 2019).

Moreover, capacities of strategic and crisis communications in the Baltics should be planned with built-in redundancy and strengthened through trustful co-operation and resource-sharing between state authorities, media, CSOs and private businesses. Additionally, segment-focused opinion-leaders should be identified, trained, motivated for and involved in planning practical crisis preparedness on local and national levels. A team-of-teams model should be considered as feasible practical concept for supporting multi-layered cross-sectoral networking between disinformation experts, practitioners, researchers, journalists and government officials. Activities like the "Resilience League" – an international cooperation platform for experts and young professionals to create shared experiences, obtain new practical knowledge and develop innovative methods for effectively counteracting hostile influence – can certainly help to introduce that kind of thinking into the Baltic environment.[132] Professional networking can help shape values and prospects of younger generations while properly planning lifelong learning activities for retired citizens to maintain resilience of and within the Baltic societies in the future.

A team-of-teams model should be considered as feasible practical concept for supporting multi-layered cross-sectoral networking

Given the increasing reliance on technology in information production, dissemination and consumption, governmental and non-governmental experts in the Baltics should start explanatory campaigns on the EU's Digital Services Act that will enter into force from 1 January 2024. It will bring a sweeping change to the online environment as the law provides a set of powerful tools that can be used to tackle online disinformation in the EU member states.[133] As this legal act is an important framework for many stakeholders on shaping information security and the media landscape in the Baltics, respective actors should have sufficient time and other recourses to adopt or redesign their modus operandi according to possibilities or limitations stipulated in the act. Moreover, civil society and independent media should increase their vigilance on the plausible negative impact of digital media on democratic developments.[134] More attention should be paid on avoiding self-censorship in free media and among intellectual communities. Additionally, special attention should be paid to the adaptation of the EU's Digital Markets Act in the light of changing workflows under the effects of AI-enabled systems.[135] The community of practitioners and policymakers involved in mitigating disinformation risks and minimising socio-psychological consequences of information disorders, should pay close attention to predicting future trends in tomorrow's disinformation environment, including expedited technological developments and the merger of sophisticated methods to recognise and manipulate human emotions.[136] Moreover, given the ongoing securitisation of the media environment, re-shaping the media and increasing information literacy requires forward-looking agility for creating new types of dynamic coalitions between various stakeholders, including decision-makers, security experts, researchers, fact-checkers, educators and journalists.[137]

The community of practitioners and policymakers should pay close attention to predicting future trends in tomorrow's disinformation environment

[132] "Europe United – Germany and Estonia join forces to combat online disinformation," Federal Foreign Office of Germany, Foreign & European Policy, 19 December 2019.

[133] "The Digital Services Act package," European Commission, Policies, last accessed 18 August 2022.

[134] Philipp Lorenz-Spreen et al., "Digital Media and Democracy: A Systematic Review of Causal and Correlational Evidence Worldwide," *SocArXiv*, 14 April 2022.

[135] Christoph Trattner et al., "Responsible media technology and AI: challenges and research directions," *AI and Ethics*, 20 December 2021.

[136] Jan Nicola Beyer and Lena-Maria Böswald, *On the radar: Mapping the tools, tactics, and narratives of tomorrow's disinformation environment* (Democracy Reporting International, July 2022).

[137] Divina Frau-Meigs, "How Disinformation Reshaped the Relationship between Journalism and Media and Information Literacy (MIL): Old and New Perspectives Revisited," *Digital Journalism* 10, no. 5 (14 July 2022): 912–922.

Result-oriented training courses on cognitive security (including preventing and countering disinformation, the role of critical thinking in decision-making, etc.) should be gradually embedded in formal and informal education activities across the Baltics, taking into account stakeholder-tailored operationalisation and the best international practices as well as thelocal context.[138] Moreover, such activities should be accessible not just for vulnerable groups, but all citizens as an integral part of either compulsorily education or self-development. At the same time, the quality of the training syllabus should be verified by disinformation experts in order to avoid delivering superficial materials without any practical outcomes. Moreover, educational activities should reach beyond traditional media literacy and address issues of information security, critical thinking, psychological mindsets and biases, as well as give practical tools to develop an operational ability to resist disinformation at individual and community levels. Internationally validated practices should be studied while considering the Baltic context as appropriate.[139]

Result-oriented training courses on cognitive security should be gradually embedded in formal and informal education activities across the Baltics

All debiasing-oriented interventions should be research-driven and based on a profound understanding of disinformation psychology.[140] Simplified debunking must be recognised as an ineffective, obsolete practice of wasting resources and having potentially toxic side effects, but also properly planned and executed pre-bunking, i.e. prophylactic measures to be developed and implemented to ensure long-lasting effects within the Baltics societies.[141] The measures should be designed by taking into account their reliability and possible backfire effect.[142] It requires comprehensive co-operation between various sectors and stakeholders, including whole-of-industry approach to combating social media manipulations.[143]

Considering the impact of the COVID-19 pandemic, as well as recent developments on information landscape, including implications of Russia's war against Ukraine and confrontation with the broader West, the cross-sectoral insights from this report suggest the need pay greater attention to multi-layered co-operation between all sectors (including research, communication and support) across the Baltics:

- within the government, i.e., inter-agency and between national and regional / local authorities;
- between the governments and academia, research institutions and think-tanks;
- between the governments and other authorities with the civil society organisations and volunteers;
- between the business sector and civil society;
- between media sector and academia;
- between civil society and media.

[138] Alice Marwick et al., *Critical Disinformation Studies: A Syllabus* (Center for Information, Technology, and Public Life, University of North Carolina, 2021); Solvita Denisa-Liepniece, *Media Literacy Sector mapping in Georgia, Latvia, Moldova and Ukraine. Latvia, Country Report* (Baltic Centre for Media Excellence, 2021).

[139] Paolo Celot (ed.), *Media Coach: How to become a media literacy coach* (European Media Coach Initiative, 2021).

[140] Stephan Lewandowsky et al., "Misinformation and Its Correction: Continued Influence and Successful Debiasing," *Psychological Science in the Public Interest* 13, no. 3 (December 2021): 106–131; Gordon Pennycook and David G. Rand, "The Psychology of Fake News," *Trends in Cognitive Sciences* 25, no. 5 (1 May 2021): 388–402.

[141] Man-pui Sally Chan et al., "Debunking: A Meta-Analysis of the Psychological Efficacy of Messages Countering Misinformation," *Psychological Science* 28, no. 11 (12 September 2017): 1531–1546; Li Qian Tay et al., "A comparison of prebunking and debunking interventions for implied versus explicit misinformation," *British Journal of Psychology* 113, no. 3 (August 2022): 591–607; Paul Butcher and Alberto-Horst Neidhardt, *From debunking to prebunking: How to get ahead of disinformation on migration in the EU* (Brussels: Foundation for European Progressive Studies, 2021); Courtney D. Boman, "Examining characteristics of prebunking strategies to overcome PR disinformation attacks," *Public Relations Review* 47, no. 5 (December 2021): 102105; Jon Roozenbeek, Sander van der Linden, and Thomas Nygren, "Prebunking interventions based on "inoculation" theory can reduce susceptibility to misinformation across cultures," *The Harvard Kennedy School Misinformation Review* 1, no. 2 (January 2020): 1–23.

[142] Briony Swire-Thompson et al., "Backfire effects after correcting misinformation are strongly associated with reliability," *Journal of Experimental Psychology: General* 151, no. 7 (July 2022): 1655–1665.

[143] Sebastian Bay et al., *Social Media Manipulation 2021/2022: Assessing the Ability of Social Media Companies to Combat Platform Manipulation* (Riga: NATO Strategic Communications Centre of Excellence, 2022).

This multi-layered cross-sectoral cooperation should be focused on strengthening political and social institutions as well as developing human capital.

Being an important part of democracy's resilience, politicians, policymakers and government officials must be properly educated in various practical aspects of resilience and crisis preparedness to maintain clearer boundaries between political, governmental, crisis and strategic communications while addressing members of the public. Moreover, politicians and policymakers should learn more about the contemporary challenges of media policy in order to strengthen national media systems in the Baltics.[144]

Ignorance cannot protect you, shared knowledge can

Amid the ongoing war in Ukraine and thinking of possible security crises in the future — and given their historical background, geographic location, as well as socio-political, socio-economic and socio-psychological peculiarities — the Baltic states should study and then operationalise the information-related factors for raising the level of societal preparedness for rapid mobilisation during a multifaceted crisis (e.g., one that encompasses war, regional instability, pandemic, environmental disaster, etc.). Introducing new behavioural norms and patterns that support resilience in such crises requires strategic thinking and reliance on best research-based international practices that should be smartly adopted in the Baltic states.[145]

Although there are some nation-specific differences between the situation in Estonia, Latvia and Lithuania, the overall picture of common challenges remains quite similar. Each country makes efforts in raising information threat awareness and increasing its systemic preparedness through a better connectivity between state and non-state actors. Therefore, the Baltic states in general, and various sectoral stakeholders in particular, should benefit from pan-Baltic connectivity and co-operation in the field of resilience, including disinformation domain, but not limited to it. To paraphrase a widely known adage: ignorance cannot protect you, shared knowledge can.

[144] Ragne Kõuts-Klemm, Anda Rožukalne, and Deimantas Jastramskis, "Resilience of national media systems: Baltic media in the global network environment," *Journal of Baltic Studies*, 26 July 2022.

[145] Kathryn M. Connor and Jonathan R. T. Davidson, "Development of a new resilience scale: The Connor-Davidson resilience scale (CD-RISC)," *Depression and Anxiety* 18, no. 2 (2003): 76–82; Dmitry Leykin et al., "Conjoint community resiliency assessment measure-28/10 items (CCRAM28 and CCRAM10): A self-report tool for assessing community resilience," *American Journal of Community Psychology* 52, no. 3–4 (2013): 313–323; Hadas Marciano et al., "Hope and Fear of Threats as Predictors of Coping with Two Major Adversities, the COVID-19 Pandemic and an Armed Conflict," *International Journal of Environmental Research and Public Health* 19, no. 3 (20 January 2022): 1123.

List of References

Andressoo, Urmo, and Mait Kraun. "Hiinlased ostsid Eesti suurima kinoäri [The Chinese bought the largest cinema company in Estonia]." *Äripäev*, 23 January 2017. https://www.aripaev.ee/borsiuudised/2017/01/23/hiinlased-ostsid-forum-cinemas-emafirma-ligi-miljardi-eest.

Andriukaitis, Lukas. *Russian Propaganda Efforts in The Baltics and the Wider Region.* Vilnius: Vilnius Institute for Policy Analysis, 2020. http://eia.libis.lt/show.php?item=russian_propaganda_e.

Applebaum, Anne, and Peter Pomerantsev. "How to put out democracy's dumpster fire." *The Atlantic*, 11 March 2021. https://www.theatlantic.com/magazine/archive/2021/04/the-internet-doesnt-have-to-be-awful/618079/.

Arold, Uku. "Põhjala ja Balti riikide psühholoogilise kaitse süsteemide kontseptuaalsed ja praktilised alused [Conceptual and Practical Foundations of the Psychological Defence Systems of Nordic and Baltic States]." Master's thesis, Estonian Academy of Security Sciences, 2021. https://digiriiul.sisekaitse.ee/handle/123456789/2698.

Baltic Centre for Media Excellence. "Our work. Research." Last accessed 18 August 2022. https://bcme.eu/en/our-work/research.

"Baltics, Poland turn to social media networks over Russian disinformation." *The Baltic Times*, 28 February 2022. https://www.baltictimes.com/baltics__poland_turn_to_social_media_networks_over_russian_disinformation/.

Baltnews.lv. "Rubrika "Vojna s pamyatnikami" [Rubric "War on Monuments"]." Last accessed 18 August 2022. https://lv.baltnews.com/trend/pamyatniki.

Bankauskaitė, Dalia. "Disinformation about history leads to disinformation about the present." *Start2Think*, last accessed 18 August 2022. https://start2think.info/disinformation-about-history-article/.

—. "Propaganda targets Baltic energy independence." *StopFake.org*, 23 January 2018. https://www.stopfake.org/en/propaganda-targets-baltic-energy-independence/.

Bankauskaitė, Dalia, and Dominykas Milasius. "The Smart Power of Lithuanian Foreign Policy." Center for European Policy Analysis, 27 April 2022. https://cepa.org/the-smart-power-of-lithuanian-foreign-policy.

Barisa-Sermule, Liene. "Fake News kingpin kept behind bars." *LSM (Latvian Public Broadcasting)*, 7 September 2018. https://eng.lsm.lv/article/society/crime/fake-news-kingpin-kept-behind-bars.a291475/.

Bay, Sebastian, Rolf Fredheim, Tetiana Haiduchyk, and Anton Dek. *Social Media Manipulation 2021/2022: Assessing the Ability of Social Media Companies to Combat Platform Manipulation*. Riga: NATO Strategic Communications Centre of Excellence, 2022. https://stratcomcoe.org/publications/social-media-manipulation-20212022-assessing-the-ability-of-social-media-companies-to-combat-platform-manipulation/242.

Bayer, Judit, Bernd Holznagel, Katarzyna Lubianiec, Adela Pintea, Josephine B. Schmitt, Judit Szakács, and Erik Uszkiewicz. *Disinformation and propaganda: impact on the functioning of the rule of law and democratic processes in the EU and its Member States. 2021 update.* Brussels: European Parliament, April 2021. https://www.europarl.europa.eu/RegData/etudes/STUD/2021/653633/EXPO_STU(2021)653633_EN.pdf.

Bērziņa, Ieva. "Political Trust and Russian Media in Latvia." *Journal on Baltic Security* 4, no. 2 (December 2018): 18. http://dx.doi.org/10.2478/jobs-2018-0008.

Bessmertnyj Polk Riga. "Bessmertnyj Polk Riga [Immortal Regiment Riga]." Last accessed 18 August 2022. http://polk.lv.

Beyer, Jan Nicola, and Lena-Maria Böswald. *On the radar: Mapping the tools, tactics, and narratives of tomorrow's disinformation environment.* Democracy Reporting International, July 2022. https://democracy-reporting.org/en/office/global/publications/new-report-tools-tactics-stories-mapping-tomorrows-disinformation-environment.

Bleyer-Simon, Konrad, Elda Brogi, Roberta Carlini, Danielle Da Costa Leite Borges, Iva Nenadic, Marie Palmer, Pier Luigi Parcu, Matteo Trevisan, Sofia Verza, and Maria Zuffova. *Monitoring media pluralism in the digital era: application of the Media Pluralism Monitor in the European Union, Albania, Montenegro, the Republic of North Macedonia, Serbia and Turkey in the year 2021*. San Domenico di Fiesole: European University Institute, 2022. https://cadmus.eui.eu/bitstream/handle/1814/74712/CMPF_MPM2021_final-report_QM-05-22-168-EN-N.pdf?sequence=1&isAllowed=y.

Boman, Courtney D. "Examining characteristics of prebunking strategies to overcome PR disinformation attacks." *Public Relations Review* 47, no. 5 (December 2021): 102105. https://doi.org/10.1016/j.pubrev.2021.102105.

Bradshaw, Samantha, and Philip N. Howard. *The Global Disinformation Order. 2019 Global Inventory of Organised Social Media Manipulation.* Oxford: University of Oxford, 2019.

Brikmane, Zane. "Pētījumaa iniciatorus šokē intelektuālā īpašuma pirātisms Latvijā. Kā cīņā ar to sokas pašmāju autoriem? [The initiators of the study are shocked by intellectual property piracy in Latvia. How do local authors cope with this?]." *LSM (Latvian Public Broadcasting)*, 13 August 2020. https://www.lsm.lv/raksts/kultura/kulturtelpa/petijuma-iniciatorus-soke-intelektuala-ipasuma-piratisms-latvija-ka-cina-ar-to-sokas-pasmaju-autoriem.a370414/.

Burton, Christopher G., Bijan Khazai, Johannes Anhorn, Jairo Valcárcel, and Diana Contreras. *Resilience Performance Scorecard (RPS) Methodology. Version 1.6*. GEM Foundation, September 2017. https://www.preventionweb.net/files/57083_gemrpsmethodologypublished.pdf.

Butcher, Paul, and Alberto-Horst Neidhardt. *From debunking to prebunking: How to get ahead of disinformation on migration in the EU*. Brussels: Foundation for European Progressive Studies, 2021. https://www.epc.eu/content/PDF/2021/Disinformation___Migration_2021_final_single.pdf.

Cabinet of Ministers of the Republic of Latvia. "Kārtība, kādā tiek nodrošināta informācijas un komunikācijas tehnoloģiju sistēmu atbilstība minimālajām drošības prasībām [Procedures for the Ensuring Conformity of Information and Communication Technologies Systems to Minimum Security Requirements]." Likumi.lv (Legal Acts of the Republic of Latvia), 28 July 2015. https://likumi.lv/ta/id/275671-kartiba-kada-tiek-nodrosinata-informacijas-un-komunikacijas-tehnologiju-sistemu-atbilstiba-minimalajam-drosibas-prasibam.

Celot, Paolo (ed.). *Media Coach: How to become a media literacy coach.* European Media Coach Initiative, 2021.

Central Electoral Commission of the Republic of Lithuania. "Politinės kampanijos dalyviai [Participants of the political campaign]." Last accessed 18 August 2022. https://www.vrk.lt/politines-kampanijos-dalyviai-2020-sei.

Central Statistical Bureau of the Republic of Latvia. *Latvijas* ārējā *tirdzniecība. Svarīgākās preces un partneri 2021. gadā [Foreign Trade of Latvia: Main Commodities and Trade Partners, 2021]*. Riga: Central Statistical Bureau, 2022. https://admin.stat.gov.lv/system/files/publication/2022-02/Nr_16_Areja_tirdznieciba_preces-partneri_2021gada_%2821_04q%29_LV.pdf.

—. "Registered religious congregations by denomination at the end of year 19902020." Official statistics portal. Last accessed 18 August 2022. https://data.stat.gov.lv/pxweb/en/OSP_PUB/STAR Legal Acts of the Republic of Latvia T__IZG__KU__KUR/KUR010/table/tableViewLayout1/.

Centre for Sustainable Peace and Democratic Development and UNDP-ACT. "SCORE Ukraine. Methodology." Last accessed 18 August 2022. https://app.scoreforpeace.org/en/ukraine/methodology.

Cepurītis, Māris, Ivo Juurvee, Austris Keišs, Diana Marnot, Belén Carrasco Rodríguez, and Scott Ruston. *Russia's Footprint in The Nordic-Baltic Information Environment.* Riga: NATO Strategic Communication Centre of Excellence, 2018. https://stratcomcoe.org/publications/download/russias_footprint_nb8_2020_nato_stratcom_coe.pdf.

Chan, Man-pui Sally, Christopher R. Jones, Kathleen Hall Jamieson, and Dolores Albarracín. "Debunking: A Meta-Analysis of the Psychological Efficacy of Messages Countering Misinformation." *Psychological Science* 28, no. 11 (12 September 2017): 1531–1546. https://doi.org/10.1177/0956797617714579.

Connor, Kathryn M., and Jonathan R. T. Davidson. "Development of a new resilience scale: The Connor-Davidson resilience scale (CD-RISC)." *Depression and Anxiety* 18, no. 2 (2003): 76–82. https://doi.org/10.1002/da.10113.

Constitution Protection Bureau of the Republic of Latvia. *Annual Public Report of the Constitution Protection Bureau of the Republic of Latvia (SAB).* Riga: Constitution Protection Bureau, 2021. https://www.sab.gov.lv/files/Public_report_2021.pdf.

Constitutional Court of the Republic of Lithuania. "On the actions of Seimas member Mindaugas Bastys. Conclusion." Constitutional Court, Case no. 12/2017, 22 December 2017. https://lrkt.lt/en/court-acts/search/170/ta1781/content.

Damarad, Volha, and Andrei Yeliseyeu. *Disinformation Resilience in Central and Eastern Europe.* Kyiv: Ukrainian Prism, 2018. http://prismua.org/en/dri-cee/.

Debunk EU. "About Debunk EU." Last accessed 18 August 2022. https://debunk.eu/about-debunk.

"Debunk EU: Latvia had the widest spread of COVID-19 related disinformation in May." *Delfi*, 11 June 2020. https://www.delfi.lt/en/politics/debunk-eu-latvia-had-the-widest-spread-of-covid-19-related-disinformation-in-may.d?id=84505739.

Delfi. "Sari "Faktikontroll" [Serie "Fact Check"]." Last accessed 18 August 2022. https://www.delfi.ee/teemalehed/faktikontroll.

Deloitte Center for Technology, Media and Telecommunications. *Digital media trends survey, 14th edition. COVID-19 accelerates subscriptions and cancellations as consumers search for value.* Deloitte Development LLC, 2020. https://www2.deloitte.com/content/dam/insights/us/articles/6456_digital-media-trends-covid/DI_Digital-media-trends-14th-edition.pdf.

Denisa-Liepniece, Solvita. *Media Literacy Sector mapping in Georgia, Latvia, Moldova and Ukraine. Latvia, Country Report.* Baltic Centre for Media Excellence, 2021. https://bcme.eu/upload/projects/550/ML_Latvia_Country_Report_2021.pdf.

—. *Sazvērestības teorija [Conspiracy theory]*. Riga: Latvijas Mediji, 2022.

—. *Zubami "Shchelk" ili Volk manipulyator*. Chișinău: Vidzeme University of Applied Sciences, 2019.

Denisa-Liepniece, Solvita, and Dmitri Teperik. "Local Russian-language Journalism in the Baltics: Challenges and Perspectives for Building Resilient Communities of Media Professionals." ICDS Policy Paper, March 2022. https://icds.ee/en/local-russian-language-journalism-in-the-baltics-challenges-and-perspectives-for-building-resilient-communities-of-media-professionals/.

Donauskaitė, Džina, Madara Fridrihsone, Miglė Krancevičiūtė, Aija Krūtaine, Alina Lastovska, Piret Reiljan, and Anastasija Tetarenko. *Baltic Media Health Check 2019–2020. The Media After Covid: Finding strategies to survive and thrive.* Riga/Tallinn/Vilnius: SSE Riga, November 2020. https://www.sseriga.edu/baltic-media-health-check-2020.

e-Governance Academy. "National Cyber Security Index – Estonia." Last accessed 18 August 2022. https://ncsi.ega.ee/country/ee/.

—. "National Cyber Security Index – Latvia." Last accessed 18 August 2022. https://ncsi.ega.ee/country/lv/312/#details.

—. "National Cyber Security Index. Methodology." Last accessed 18 August 2022. https://ncsi.ega.ee/methodology/.

Economic Complexity Observatory. "Lithuania (trade data)." Last accessed 18 August 2022. https://oec.world/en/profile/country/ltu.

Edgemon, Lesley, Carol Freeman, Carmella Burdi, John Hutchison, Karen Marsh, and Kyle Pfeiffer. *Community Resilience Indicator Analysis: County-Level Analysis of Commonly Used Indicators from Peer-Reviewed Research, 2020 Update.* Argonne National Laboratory, Federal Emergency Management Agency, 2020. https://www.fema.gov/sites/default/files/2020-11/fema_community-resilience-indicator-analysis.pdf.

ERR. "ERRi meediapädevuse projekt "Meediataip" [ERR's media literacy project "Meediataip"]." Last accessed 18 August 2022. https://novaator.err.ee/k/meediataip.

Estonian Foreign Intelligence Service. "Security environment assessment." Last accessed 18 August 2022. https://www.valisluureamet.ee/assessment.html.

Estonian Internal Security Service. "Aastaraamatu väljaandmise traditsiooni ajalugu ja eesmärk [Annual reviews: History and Goals of the Tradition of Annual Reviews]." Last accessed 18 August 2022. https://kapo.ee/et/aastaraamatud/.

European Centre of Excellence for Countering Hybrid Threats. "Publications and readings." Last accessed 18 August 2022. https://www.hybridcoe.fi/publications-and-readings/.

European Commission, Directorate General for Trade. "EU27 Trade in Goods Services by partner (2020, excluding intra-EU trade)." Last updated 20 April 2022. https://trade.ec.europa.eu/doclib/docs/2006/september/tradoc_122530.pdf.

European Commission. "The Digital Services Act package." Policies. Last accessed 18 August 2022. https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package.

European Parliament. "Välismaine ettevõtete ülevõtmine Covid-19 kriisi ajal: saadikud nõuavad võrdseid võimalusi [Foreign takeovers in Covid-19 crisis: MEPs push for level-playing field]." European Parliament, 24 June 2020. https://www.europarl.europa.eu/news/et/headlines/economy/20200618STO81512/valismaine-ettevotete-ulevotmine-saadikud-nouavad-vordseid-voimalusi.

European Parliament and the Council of the European Union. "Regulation (EU) No. 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC." *Official Journal of the European Union,* L 257/73, 28 August 2014. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014R0910.

Eurostat. "How many people verified online information in 2021?" 16 December 2021. https://ec.europa.eu/eurostat/web/products-eurostat-news/-/DDN-20211216-3.

Federal Foreign Office of Germany. "Europe United – Germany and Estonia join forces to combat online disinformation." Foreign & European Policy. 19 December 2019. https://www.auswaertiges-amt.de/en/aussenpolitik/europe/-/2289666.

FM Global. "2022 FM Global Resilience Index." Last accessed 18 August 2022. https://www.fmglobal.com/research-and-resources/tools-and-resources/resilienceindex.

Foundation for European Progressive Studies. *Resisting Foreign State Propaganda in the New Information Environment: the Case of the EU, Russia, and the Eastern Partnership Countries.* Baloži: Foundation for European Progressive Studies, Brīvības un Solidaritātes Fonds, 2016. http://appc.lv/eng/wp-content/uploads/sites/2/2016/09/Propoganda_petijums.pdf.

Frau-Meigs, Divina. "How Disinformation Reshaped the Relationship between Journalism and Media and Information Literacy (MIL): Old and New Perspectives Revisited." *Digital Journalism* 10, no. 5 (14 July 2022): 912–922. https://doi.org10.1080/21670811.2022.2081863.

Garcia, Cynthia. *The Baltic Centre For Media Excellence. A Case Study on Media Literacy as a Tool Against Russian Disinformation.* Medford, MA: Tufts University, May 2018. https://sites.tufts.edu/fletcherrussia/files/2018/09/2018-Cynthia-A.-Garcia-The-Baltic-Center-for-Media-Excellence.-A-Case-Study-on-Media-Literacy-as-a-Tool-Against-Russian-Disinformation-.pdf.

García, Juan Pablo Villar, Carlota Tarín Quirós, Julio Blázquez Soria, Carlos Galán Pascual, and Carlos Galán Cordero. *Strategic communications as a key factor in countering hybrid threats.* Brussels: European Parliament, March 2021. https://data.europa.eu/doi/10.2861/14410.

GEC Special Report: Pillars of Russia's Disinformation and Propaganda Ecosystem. Washington D.C.: U.S. Department of State, August 2020. https://www.state.gov/russias-pillars-of-disinformation-and-propaganda-report.

Gold, Josh. "Estonia as an international cybersecurity leader." E-Estonia, 21 August 2019. https://e-estonia.com/estonia-as-an-international-cybersecurity-leader/.

Government Office of the Republic of Estonia. "Strategic communication." Last updated 8 February 2022. https://riigikantselei.ee/en/strategic-communication.

"Grand duchy of Lithuania." *Encyclopaedia Britannica*, 9 February 2016. https://www.britannica.com/place/grand-duchy-of-Lithuania.

Hajdu, Dominika, Jana Kazaz, Katarina Klingová, and Michal Kortiš. *GLOBSEC Trends 2022: CEE amid the War in Ukraine.* Bratislava: Democracy and Resilience Centre at GLOBSEC, 2022. https://www.globsec.org/wp-content/uploads/2022/05/GLOBSEC-Trends-2022_single-pages.pdf.

Hajdu, Dominika, Katarína Klingová, Daniel Milo, and Miroslava Sawiris. *GLOBSEC Trends 2021: Central & Eastern Europe one year into the pandemic*. Bratislava: Democracy and Resilience Centre at GLOBSEC, June 2021. https://www.globsec.org/wp-content/uploads/2021/06/GLOBSEC-Trends-2021_final.pdf.

Hassain, Jon. *Disinformation in Democracies: Improving Societal Resilience to Disinformation*. Riga: NATO Strategic Communications Centre of Excellence, March 2022. https://stratcomcoe.org/publications/disinformation-in-democracies-improving-societal-resilience-to-disinformation/241.

Helmus, Todd C., Elizabeth Bodine-Baron, Andrew Radin, Madeline Magnuson, Joshua Mendelsohn, William Marcellino, Andriy Bega, and Zev Winkelman. *Russian Social Media Influence: Understanding Russian Propaganda in Eastern Europe.* Santa Monica, CA: Rand Corporation, 2018. https://www.rand.org/content/dam/rand/pubs/research_reports/RR2200/RR2237/RAND_RR2237.pdf.

Himma, Marju. "Uuring: ERRi usaldusväärsus kasvab, eriti vene inimeste hulgas [Survey: trust in ERR is growing, especially among Russian people]." *ERR*, 31 May 2019. https://www.err.ee/947805/uuring-erri-usaldusvaarsus-kasvab-eriti-vene-inimeste-hulgas.

Humprecht, Edda, Frank Esser, and Peter Van Aelst. "Resilience to Online Disinformation: A Framework for Cross-National Comparative Research." *The International Journal of Press/Politics* 25, no. 3 (July 2020): 493–516. https://doi.org/10.1177/1940161219900126.

International Centre for Defence and Security. "Estonian National Defence Course (ENDC)." Last accessed 18 August 2022. https://krkk.icds.ee/en/.

International Republican Institute, Center for Insights in Survey Research. "Public Opinion Poll: Latvia, January 10 - February 2, 2020." Last accessed 18 August 2022. https://www.iri.org/wp-content/uploads/legacy/iri.org/latvia_slide_deck_ltvto_be_published_0.pdf.

International Telecommunication Union. "Global Cybersecurity Index." Last accessed 18 August 2022. https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx.

Information System Authority of the Republic of Estonia. "Eakad saavad aasta lõpuni küberturvalisuse nõu infoliinilt [Until the end of this year, senior citizens can call the helpline for advice on cymbersecurity]." 16 November 2020. https://www.ria.ee/et/uudised/eakad-saavad-aasta-lopuni-kuberturvalisuse-nou-infoliinilt.html.

—. "Publications – Yearbooks." Last accessed 18 August 2022. https://www.ria.ee/en/information-system-authority/publications.html.

—. "RIA juhend ja videod aitavad ettevõtteil ennast küberruumis kaitsta [RIA's handbook and videos help companies protect themselves in cyberspace]." 8 April 2020. https://www.ria.ee/et/uudised/ria-juhend-ja-videod-aitavad-ettevotteil-ennast-kuberruumis-kaitsta.html.

Janeliūnas, Tomas. "The Long Shadow of a Nuclear Monster: Lithuanian responses to the Astravyets NPP in Belarus." ICDS Analysis, March 2021. https://icds.ee/wp-content/uploads/2021/03/ICDS_Analysis_The_Long_Shadow_of_a_Nuclear_Monster_Tomas_Janeliunas_March_2021.pdf.

Jemberga, Sanita. "Dārgā policija, sveicieni no (vēl dzīvas) stervas [Dear police, greetings from a (still alive) bitch]." *Delfi*, 17 December 2020. https://www.delfi.lv/news/versijas/sanita-jemberga-darga-policija-sveicieni-no-vel-dzivas-stervas.d?id=51729509.

Jin, Michael X., Sangita Rajan, Carlos E. Gary Bicas, Max Hao, Letian Dong, Beckett Mufson, and Imran Hafiz. "Novel Validated Index for the Measurement of Disinformation Susceptibility at the County Level." *Cureus* 13, no. 5: e15305. https://doi.org/10.7759%2Fcureus.15305.

Jõesaar, Andres, Anda Rožukalne, and Deimantas Jastramskis. "The role of media in the Baltics. To trust or not to trust?" Baltic Centre for Media Excellence, last accessed 18 August 2022. https://bcme.eu/upload/products/518/PRESENTATION%20Baltic%20Media%20Research.pdf.

Jokinen, Janne, and Magnus Normark. *Hybrid threats from non-state actors: A taxonomy.* Helsinki: The European Centre of Excellence for Countering Hybrid Threats, June 2022. https://www.hybridcoe.fi/wp-content/uploads/2022/05/20220609-Hybrid-CoE-Research-Report-6-Non-state-actors-WEB.pdf.

Kantar Emor. "Eesti elanikud usaldavad enim ETVd ja ERRi uudisportaali [ETV and ERR are the most trusted media channels among residents of Estonia]." Press Release, 30 March 2020. https://www.kantaremor.ee/pressiteated/eesti-elanikud-usaldavad-enim-etvd-ja-erri-uudisportaali.

Kaprāns, Mārtiņš, and Inta Mieriņa. *Ideological Polarization in Baltic Societies. A Cross-National Survey Report.* Riga: University of Latvia, 2019. http://fsi.lu.lv/userfiles/file/2019_ideological_polarization_report.pdf.

Karlsen, Geir Hågen. "Divide and rule: ten lessons about Russian political influence activities in Europe." *Palgrave Communications* 5 (8 February 2019). https://www.nature.com/articles/s41599-019-0227-8.

Khrennikov, Ilya. "Netflix Joins Putin Ally's National Media for Russia Rollout." *Bloomberg*, 2 September 2020. https://www.bloomberg.com/news/articles/2020-09-02/netflix-joins-putin-ally-s-national-media-for-russia-rollout.

Kont, Hannes. “Synchronization with continental Europe.” Elering, updated July 2022. https://elering.ee/en/synchronization-continental-europe.

Kõuts-Klemm, Ragne. Anda Rožukalne, and Deimantas Jastramskis. “Resilience of national media systems: Baltic media in the global network environment.” *Journal of Baltic Studies*, 26 July 2022. https://doi.org/10.1080/01629778.2022.2103162.

“Krievija gribējusi ierīkot novērošanas kameras ap Alūksnes ezeru. Tas ļautu izspiegot blakus esošo armijas bāzi [Russia wanted to install surveillance cameras around Lake Alūksne. This would enable spying on a nearby military base].” *TV3.lv*, 31 May 2020. https://zinas.tv3.lv/latvija/neka-personiga/krievija-gribejusi-ierikot-noverosanas-kameras-ap-aluksnes-ezeru-tas-lautu-izspiegot-blakus-esoso-armijas-bazi/.

Kruuda, Lennart. “Eesti aasta ettevõte müüdi 40 miljoni euroga hiinlastele [Estonian Company of the year sold to Chinese for 40 million euros].” *Postimees*, 3 January 2018. https://majandus24.postimees.ee/4363085/eesti-aasta-ettevote-muudi-40-miljoni-euroga-hiinlastele.

Kudors, Andis, ed. *Fortress Russia: Political, Economic, and Security Development in Russia Following the Annexation of Crimea and its Consequences for the Baltic States.* Riga: The Centre for East European Policy Studies, University of Latvia Press, 2016. http://appc.lv/eng/wp-content/uploads/sites/2/2016/02/vaks-ar-tekstu.pdf.

La Torre, Ilaria. *The Baltic’s response to Russia’s Threat – How Estonia, Latvia and Lithuania reacted to the recent actions of the Russian federation.* Brussels: European Army Interoperability Centre, 2020. https://finabel.org/the-baltics-response-to-russias-threat-how-estonia-latvia-and-lithuania-reacted-to-the-recent-actions-of-the-russian-federation/.

Latvian Media Ethics Council. “Latvijas Mediju ētikas padome dokumenti [Latvian Media Ethics Council documents].” Last accessed 18 August 2022. https://www.lmepadome.lv/par-mums/dokument.

Latvian State Security Service. *Annual Report on the activities of Latvian State Security Service in 2019.* Riga: Latvian State Security Service, March 2020. https://vdd.gov.lv/uploads/materials/1/en/annual-report-2019.pdf.

Lessenski, Marin. “Media Literacy Index 2021.” Open Society Institute – Sofia, 14 March 2021, https://osis.bg/?p=3750&lang=en.

“Levits komentē Lato Lapsas grāmatā “Viltvārdis” izteiktās šaubas par viņa biogrāfiju [Levits comments on the doubts expressed in Lato Lapsa’s book “Viltvārdis” about his biography].” *Apollo.lv*, 16 July 2020. https://www.apollo.lv/7018793/levits-komente-lato-lapsas-gramata-viltvardis-izteiktas-saubas-par-vina-biografiju.

Lewandowsky, Stephan, Ullrich K. H. Ecker, Colleen M. Seifert, Norbert Schwarz, and John Cook. “Misinformation and Its Correction: Continued Influence and Successful Debiasing.” *Psychological Science in the Public Interest* 13, no. 3 (December 2021): 106–131. https://doi.org/10.1177/1529100612451018.

Leykin, Dmitry, Mooli Lahad, Odeya Cohen, Avishay Goldberg, and Limor Aharonson-Daniel. “Conjoint community resiliency assessment measure-28/10 items (CCRAM28 and CCRAM10): A self-report tool for assessing community resilience.” *American Journal of Community Psychology* 52, no. 3–4 (2013): 313–323. https://doi.org/10.1007/s10464-013-9596-0.

“Lithuanian armed forces analysts: disinformation has expanded, especially about the migration crisis.” *Baltic News Network*, 15 December 2021. https://bnn-news.com/lithuanian-armed-forces-analysts-disinformation-has-expanded-especially-about-the-migration-crisis-230928.

Lorenz-Spreen, Philipp, Lisa Oswald, Stephan Lewandowsky, and Ralph Hertwig. “Digital Media and Democracy: A Systematic Review of Causal and Correlational Evidence Worldwide.” *SocArXiv*, 14 April 2022. https://osf.io/preprints/socarxiv/p3z9v/.

Lucas, Edward, Ben Dubow, James Lamond, Jake Morris, Corina Rebegea, and Vera Zakem. *Post-Mortem: Russian and Chinese COVID-19 Information Operations.* Washington DC: Center for European Policy Analysis, 2021. https://cepa.org/post-mortem-russian-and-chinese-covid-19-information-operations/.

Lucas, Edward, Ben Hodges, and Carsten Schmiedl. “Close to the Wind: What Russia Wants.” Center for European Policy Analysis, 9 September 2021. https://cepa.org/baltic-sea-security-what-russia-wants/.

Maaten, Epp, and Toomas Vaks (eds.). *National Cyber Security in Practice.* Tallinn: E-riigi Akadeemia, 2020. https://ega.ee/publication/national-cyber-security-handbook.

Marciano, Hadas, Yohanan Eshel, Shaul Kimhi, and Bruria Adini. “Hope and Fear of Threats as Predictors of Coping with Two Major Adversities, the COVID-19 Pandemic and an Armed Conflict.” *International Journal of Environmental Research and Public Health* 19, no. 3 (20 January 2022): 1123. https://doi.org/10.3390/ijerph19031123.

Martin-Rozumiłowicz, Beata, and Rasto Kužel. *Social Media, Disinformation and Electoral Integrity*. Arlington, VA: International Foundation for Electoral Systems, 2019. https://www.ifes.org/sites/default/files/ifes_working_paper_social_media_disinformation_and_electoral_integrity_august_2019.pdf.

Marwick, Alice, Rachel Kuo, Shanice Jones Cameron, and Moira Weigel. *Critical Disinformation Studies: A Syllabus.* Center for Information, Technology, and Public Life, University of North Carolina, 2021. http://citap.unc.edu/critical-disinfo.

McGonagle, Tarlach, Maciek Bednarski, Mariana Francese Coutinho, and Arthur Zimin. *Elections and Media in Digital Times.* Paris: UNESCO, 2019. https://unesdoc.unesco.org/ark:/48223/pf0000371486.

Merimaa, Kertti, and Krista Lepik. “Information literacy on the political agenda: An analysis of Estonian national strategic documents.” *Central European Journal of Communication* 13, no. 2 (May 2020): 183–201. https://doi.org/10.19195/1899-5101.13.2(26).3.

Michlin-Shapir, Vera, David Siman-Tov, and Nufar Shaashua. “Russia as an Information Superpower.” In *Cognitive Campaign: Strategic Intelligence Perspectives*, edited by Yossi Kuperwasser and David Siman-Tov. Tel Aviv: Institute for National Security Studies, 2019. https://www.inss.org.il/wp-content/uploads/2019/10/Memo197_e_compressed.pdf.

Miguel, Raquel. *Towards an Impact-risk Index of Disinformation: Measuring the Virality and Engagement of Single Hoaxes.* Brussels: EU Disinfo Lab, June 2022. https://www.disinfo.eu/wp-content/uploads/2022/06/20220617_IndexImpactAssessment_Final.pdf.

Ministry of Culture of the Republic of Lithuania. *Žiniasklaidos priemonių naudojimo raštingumo lygio pokyčio tyrimas [Survey on Changes of Media Literacy Level]*. Vilnius: Ministry of Culture, 2021. https://www.kulturostyrimai.lt/wp-content/uploads/2021/10/ZINIASKLAIDOS-PRIEMONIU-NAUDOJIMO-RASTINGUMO-LYGIOPOKYCIO-TYRIMAS.pdf.

Ministry of Defence of the Republic of Latvia. *Valsts Aizsardzības Koncepcija [State Defence Concept].* Riga: Ministry of Defence, October 2020. https://www.mod.gov.lv/sites/mod/files/document/AiMVAK_2020.pdf.

Ministry of Economic Affairs and Communications of the Republic of Estonia. “Riigi küberturvalisuse tagamine [Ensuring Cybersecurity].” Last accessed 18 August 2022. https://www.mkm.ee/digiriik-ja-uhenduvus/kuberturvalisus/riigi-kuberturvalisuse-tagamine.

Ministry of Education and Research of the Republic of Estonia. “Meediapädevuse nädal 2020 [Media Literacy Week 2020].” Last updated 16 February 2021. https://www.hm.ee/et/tegevused/meediapadevus/meediapadevuse-nadal-2020.

Ministry of Education and Science of the Republic of Lithuania. *Valstybinė švietimo 2013–2022 metų strategija [National Education Strategy 20132022].* Vilnius: Centre for Educational Supplies of the Ministry of Education and Science, 2014. https://www.nsa.smm.lt/wp-content/uploads/2018/04/Valstybine-svietimo-strategija-2013-2020_svietstrat.pdf.

Ministry of National Defence of the Republic of Lithuania. *Nacionalinė kibernetinio saugumo būklės ataskaita 2020 [National Cyber Security Status report for the year 2020].* Vilnius: Ministry of National Defence of Lithuania, 2021. https://vdai.lrv.lt/uploads/vdai/documents/files/2020%20m_%20Nacionalinio%20kibernetinio%20saugumo%20b%C5%ABkl%C4%97s%20ataskaita%20el_%20versija.pdf.

Mölder, Holger, and Vladimir Sazonov. “The Kremlin’s strategic narratives on the Baltic states during the COVID-19 crisis.” *Kwartalnik Bellona* 70, no. 4 (2020): 1–10. http://doi.org/10.5604/01.3001.0014.6983.

Molina, Maria D., S. Shyam Sundar, Thai Le, and Dongwon Lee. ““Fake News” Is Not Simply False Information: A Concept Explication and Taxonomy of Online Content.” *American Behavioral Scientist* 65, no. 2 (February 2021): 180–212. https://doi.org/10.1177/0002764219878224.

“Nagorno-Karabakh Conflict: A Visual Explainer.” International Crisis Group, 3 August 2022. https://www.crisisgroup.org/content/nagorno-karabakh-conflict-visual-explainer.

National Electronic Mass Media Council of Latvia. “NEPLP: Kiselyov, who is on the EU sanction list, ensures full control over RT according to the decree signed by Putin.” 7 July 2020. https://www.neplp.lv/en/article/neplp-kiselyov-who-eu-sanction-list-ensures-full-control-over-rt-according-decree-signed-putin.

—. "The court decides to maintain the NEPLP decision on restricting the distribution of 9 programmes." 12 February 2020. https://www.neplp.lv/en/article/court-decides-maintain-neplp-decision-restricting-distribution-9-programmes.

NATO Strategic Communications Centre of Excellence. "Publications." Last accessed 18 August 2022. https://stratcomcoe.org/publications.

Newman, Nic. *Journalism, Media, and Technology Trends and Predictions 2020.* Reuters Institute / University of Oxford, 2020. http://www.digitalnewsreport.org/publications/2020/journalism-media-and-technology-trends-and-predictions-2020/.

Pabriks, Artis. *Informatīvais ziņojums "Latvijas kiberdrošības stratēģija 2019.–2022. gadam" [Informational report "Latvia's cyber security strategy 2019–2022].* Riga: Ministry of Defence of the Republic of Latvia, 2019. https://www.mod.gov.lv/sites/mod/files/document/kiberstrategija.pdf.

—. "Zdravstvujte, uvazhayemyye zhiteli Latvii! [Dear residents of Latvia!]." Ministry of Defence of the Republic of Latvia. Last accessed 18 August 2022. https://www.mod.gov.lv/sites/mod/files/document/письмо_0.pdf.

Pabriks, Artis, and Andis Kudors (eds.). *The War in Ukraine: Lessons for Europe.* Riga: University of Latvia Press, 2015.

Pausch, Markus, Patricia Hladschik, Rasha Nagem, and Filip Pazderski. *Resilience Against Anti-Democratic Tendencies through Education. Competences for Democratic Culture in European Social and Youth Work.* Salzburg/Strasbourg/Toulouse/Vienna/Warsaw: Council of Europe, 2021. https://rm.coe.int/resilience-against-anti-democratic-tendencies-through-education-compet/1680a5e8f3.

Pennycook, Gordon, and David G. Rand. "The Psychology of Fake News." *Trends in Cognitive Sciences* 25, no. 5 (1 May 2021): 388–402. https://www.cell.com/trends/cognitive-sciences/fulltext/S1364-6613(21)00051-6.

Phillips, Whitney. *The Oxygen of Amplification, Better Practices for Reporting on Extremists, Antagonists, and Manipulators Online.* Data & Society Research Institute, 2018. https://datasociety.net/library/oxygen-of-amplification/.

Postimees. "Faktikontroll "Õige või vale" [Fact Check "True or Wrong"]." Last accessed 18 August 2022. https://www.postimees.ee/term/593540/faktikontroll.

Re:Baltica. "Who spreads vaccine lies in the Baltics?" *LRT*, 2 March 2021. https://www.lrt.lt/en/news-in-english/19/1355005/who-spreads-vaccine-lies-in-the-baltics.

Reisher, Jon, Charity Jacobs, and John Beasley. "Data as a Weapon: Psychological Operations in the Age of Irregular Information Threats." Modern War Institute, 5 February 2022. https://mwi.usma.edu/data-as-a-weapon-psychological-operations-in-the-age-of-irregular-information-threats.

Reynié, Dominoque, ed. *Freedoms at risk: the challenge of the century. A global survey on democracy in 55 countries.* Fondation pour l'innovation politique, January 2022. https://www.fondapol.org/en/study/freedoms-at-risk-the-challenge-of-the-century/.

Riigikogu (Parliament of the Republic of Estonia). "Eesti ekspordipoliitika põhialuste heakskiitmine [Approval of the principles of Estonian export policy]." *Riigi Teataja,* I, 92, 556 (2001). https://www.riigiteataja.ee/akt/73260.

—. "Elektroonilise side seaduse muutmise seadus 138 SE [Electronic Communications Act Amendment Act 138 SE]." *Riigi Teataja,* RT I, 33 (2020). https://www.riigiteataja.ee/akt/120052020033.

Roozenbeek, Jon, Sander van der Linden, and Thomas Nygren. "Prebunking interventions based on "inoculation" theory can reduce susceptibility to misinformation across cultures." *The Harvard Kennedy School Misinformation Review* 1, no. 2 (January 2020): 1–23. https://misinforeview.hks.harvard.edu/wp-content/uploads/2020/02/FORMATTED_globalvaccination_Jan30.pdf.

Russian Federation Embassy in Latvia. "Mezhdunarodnyj konkurs sredi zhurnalistov "Yantarnoye pero" [Amber Feather Journalism Competition]." Last accessed 18 August 2022, https://latvia.mid.ru/ru/press-centre/mezhdunarodnyy_konkurs_yantarnoe_pero/.

Saeima (Parliament of the Republic of Latvia). "Latvijas Pareizticīgās Baznīcas likums [The law of the Orthodox Church of Latvia]." Likumi.lv (Legal Acts of the Republic of Latvia), 3 December 2008. https://likumi.lv/ta/id/184626-latvijas-pareizticigas-baznicas-likums.

—. "Par Valsts aizsardzības koncepcijas apstiprināšanu [National Defence Concept]." Likumi.lv (Legal Acts of the Republic of Latvia), 24 September 2020. https://likumi.lv/ta/id/317591-par-valsts-aizsardzibas-koncepcijas-apstiprinasanu.

Seimas (Parliament of the Republic of Lithuania). "Lietuvos Respublikos visuomenės informavimo įstatymas [Law on Public Information of the Republic of Lithuania]." *Valstybės* žinios, no. 71-1706, 26 July 1996. https://www.e-tar.lt/portal/lt/legalAct/TAR.065AB8483E1E/asr.

Shestopalova, Alona. "Forgotten and Potentially Vulnerable: Why the Online Activity of Middle-Aged Women Matters During Global Information Warfare." ICDS Policy Paper, April 2022. https://icds.ee/en//download/47064330/.

Spilerman, Seymour, and Guy Stecklov. "Societal Responses to Terrorist Attacks." *The Annual Review of Sociology* 35, no. 1 (August 2009): 167–189. http://dx.doi.org/10.1146/annurev-soc-070308-120001.

State Security Department of the Republic of Lithuania and Second Investigation Department under the Ministry of National Defence of the Republic of Lithuania. *Grėsmių nacionaliniam saugumui vertinimas [National Security Threats Assessment].* Vilnius: Ministry of National Defence / State Security Department, 2020. https://www.vsd.lt/wp-content/uploads/2020/02/2020-Gresmes-LT-.pdf.

—. *National Security Threat Assessment.* Vilnius: Ministry of National Defence, 2016. https://www.vsd.lt/wp-content/uploads/2016/10/EN-2015-gresmes.pdf.

Statistics Estonia. "Estonia: Destinations 2021, Consignment 2021." Last accessed 18 August 2022, https://valiskaubandus.stat.ee/profile/country/ee/?locale=en.

Stockholm School of Economics in Riga. "Baltic Media Health Check 2018-2019 published." SSE Riga, 5 November 2019. https://www.sseriga.edu/baltic-media-health-check-2018-2019-published.

Sweney, Mark. "Netflix subscribers in Russia launch class action for loss of service." *The Guardian*, 13 April 2022. https://www.theguardian.com/media/2022/apr/13/netflix-subscribers-russia-class-action-loss-service-ukraine.

Swire-Thompson, Briony, Nicholas Miklaucic, John P. Wihbey, David Lazer, and Joseph DeGutis. "Backfire effects after correcting misinformation are strongly associated with reliability." *Journal of Experimental Psychology: General* 151, no. 7 (July 2022): 1655–1665. https://psycnet.apa.org/doi/10.1037/xge0001131.

Taleb, Nassim Nickolas. *Antifragile: Things That Gain From Disorder.* New York: Random House, 2012.

Tatham, Steve. *The Solution to Russian Propaganda is not EU or NATO Propaganda but Advanced Social Science to Understand and Mitigate its Effect in Targeted Populations.* Riga: National Defence Academy of Latvia, July 2015. https://www.naa.mil.lv/sites/naa/files/document/4_PP%2004-2015.pdf.

Tay, Li Qian, Mark J. Hurlstone, Tim Kurz, and Ullrich K. H. Ecker. "A comparison of prebunking and debunking interventions for implied versus explicit misinformation." *British Journal of Psychology* 113, no. 3 (August 2022): 591–607. https://doi.org/10.1111/bjop.12551.

Teperik, Dmitri. "Democracy, 'Alternative Reality' and Estonia's Resilience." ICDS Brief, October 2020. https://icds.ee/en/democracy-alternative-reality-and-estonias-resilience/.

—. *Kak zhiteli Elu svoj volshebnyj les ot nepravdy zashchishchali [How the inhabitants of Elu protected their magic forest from lies].* Tallinn: MTÜ Ida-Viru Noorteakadeemia, 2021.

Trattner, Christoph, Dietmar Jannach, Enrico Motta, Irene Costera Meijer, Nicholas Diakopoulos, Mehdi Elahi, Andreas L. Opdahl, Bjørnar Tessem, Njål Borch, Morten Fjeld, Lilja Øvrelid, Koenraad De Smedt, and Hallvard Moe. "Responsible media technology and AI: challenges and research directions." *AI and Ethics*, 20 December 2021. https://link.springer.com/content/pdf/10.1007/s43681-021-00126-4.pdf.

Treyger, Elina, Joe Cheravitch, and Raphael S. Cohen. *Russian Disinformation Efforts on Social Media.* Santa Monica, CA: Rand Corporation, 2022. https://www.rand.org/pubs/research_reports/RR4373z2.html.

UNCTAD Investment Policy Hub. "Lithuania. Law on the Protection of Objects of Importance to Ensuring National Security." UNCTAD Compendium of Investment Laws, 12 January 2018. https://investmentpolicy.unctad.org/investment-laws/laws/246/lithuania-law-on-the-protection-of-objects-of-importance-to-ensuring-national-security-#:~:text=The%20objective%20of%20this%20Law,of%20importance%20to%20ensuring%20national.

"Valsts iestāžu darbinieku tālruņi slepus sūtījuši datus uz serviertem Ķīņā [Phones of Latvian public servants have been secretly sending data to servers in China]." *la.lv (Latvians News)*, 28 November 2016. https://www.la.lv/valsts-iestazu-darbinieku-talruni-slepus-sutijusi-datus-uz-serveriem-kina.

Viešoji įstaiga Inovacijų agentūra [Innovation Agency Lithuania]. "Lietuvos prekių eksporto apžvalga 2021 [Overview of Lithuanian goods export 2021]." 1 March 2022. https://kc.inovacijuagentura.lt/site/binaries/content/assets/analitika/apzvalgos/2022/2021_prekiu-eksporto-apzvalga.pdf.

Voltri, Johannes. "Comparison of governmental approaches to counter Russian information influence in the Baltic states." Master's thesis, University of Tartu, 2021. https://dspace.ut.ee/handle/10062/71293.

Wang, Chih-Chien. "Fake News and Related Concepts: Definitions and Recent Research Development." *Contemporary Management Research* 16, no. 3 (2020): 145–174. https://doi.org/10.7903/cmr.20677.

Wardle, Claire, and Hossein Derakhshan. *Information Disorder. Toward an interdisciplinary framework for research and policymaking.* Strasbourg: Council of Europe, October 2017. https://rm.coe.int/information-disorder-toward-an-interdisciplinary-framework-for-researc/168076277c.

Wells II, Linton. "Cognitive-Emotional Conflict: Adversary Will and Social Resilience." *Prisma* 7, no. 2 (2017): 4–17. https://www.jstor.org/stable/10.2307/26470514.

Wilfore, Kristina. *A Digital Resilience Toolkit for Women in Politics Persisting and Fighting Back Against Misogyny and Digital Platforms' Failures*. #ShePersisted, 2022. https://secureservercdn.net/160.153.137.91/r2g.26a.myftpupload.com/wp-content/uploads/2022/06/ShePersisted_Digital_Resilience_Toolkit.pdf.

Yandex. "Transparency Report. Raskrytiye informatsii o zaprosakh [Trancparency Report. Request for disclosure of information]." Last accessed 18 August 2022. https://yandex.ru/company/privacy/transparencyreport.

RECENT ICDS PUBLICATIONS

Reports

Jermalavičius, Tomas, Max Bergmann, Peter Crail, Thomas O'Donnell, Tomas Janeliūnas, and Tõnis Idarand. Developing Nuclear Energy in Estonia: An Amplifier of Strategic Partnership with the United States? Tallinn: International Centre for Defence and Security, September 2022.

Arjakas, Merili, Hille Hanso, Kristi Raik, Peeter Raudsik, and Vladimir Sazonov. Estonia's Co-operation with the EU's Southern Neighbourhood: Strategic Objectives and Focus. Tallinn: ICDS Estonian Foreign Policy Institute, August 2022.

Jermalavičius, Tomas, Tomas Janeliūnas, Andrian Prokip, Iliya Kusa, Alan Riley, Pier Paolo Raimondi, Andrei Beliy, and Miguel Sainz de Vicuña. Geopolitics of Europe's Hydrogen Aspirations: Creating Sustainable Equilibrium or a Combustible Mix? Tallinn: International Centre for Defence and Security, May 2022.

Haugevik, Kristin, Piret Kuusik, Kristi Raik, and Niels Nagelhus Schia. Small States, Different Approaches: Estonia and Norway on the UN Security Council. Tallinn: ICDS Estonian Foreign Policy Institute, November 2021.

Teperik, Dmitri, Grigori Senkiv, Dmytro Dubov, Oleh Pokalchuk, Illia Miroshkin, Oksana Iliuk, Anastasiia Apetyk, and Larysa Snihur. Resilient Ukraine – A Delicate Mosaic? Society, Media, Security, and Future Prospects. Tallinn: International Centre for Defence and Security, November 2021.

Books

Raik, Kristi, Frank Jüris, and Bart Gaens, eds. Nordic-Baltic Connectivity with Asia via the Arctic: Assessing Opportunities and Risks. Tallinn: ICDS Estonian Foreign Policy Institute, 2021.

Policy Papers

Blockmans, Steven, and Kristi Raik. "Ukraine's Path to EU Membership: How to Turn a Geopolitical Necessity into a Viable Process." ICDS/EFPI Policy Paper, June 2022.

Shestopalova, Alona. "Forgotten and Potentially Vulnerable: Why the Online Activity of Middle-Aged Women Matters During Global Information Warfare." ICDS Policy Paper, April 2022.

Denisa-Liepniece, Solvita, and Dmitri Teperik. "Local Russian-language Journalism in the Baltics: Challenges and Perspectives for Building Resilient Communities of Media Professionals." ICDS Policy Paper, March 2022.

Analyses

Gretskiy, Igor. "A War of the Final Soviet Generation: Russia's Demography, Society, and Aggression Against Ukraine." ICDS Analysis, August 2022.

Crippa, Lorenzo. "From Rome to Kyiv, Passing Through Moscow: Russian Strategic Narratives in the Italian Public Discourse on Ukraine." ICDS Analysis, April 2022.

Gowan, Richard. "Estonia in the Security Council: A History in Three Crises." ICDS/EFPI Analysis, March 2022.

Weitz, Richard. "NATO's Hypersonic Challenge." ICDS Analysis, February 2022.

Lawrence, Tony. "Command and Control for the CSDP: A Permanent Operation Headquarters for the EU?" ICDS Analysis, January 2022.

All ICDS publications are available from https://icds.ee/category/publications

Follow us on:

ICDS.Tallinn

@ICDS _ Tallinn

ICDS-Tallinn

www.icds.ee

International Centre for Defence and Security
63/4 Narva Rd., 10120 Tallinn, Estonia
info@icds.ee

ISSN 2228-2076

ISBN 978-9916-709-03-0 (pdf)
ISBN 978-9916-709-02-3 (print)