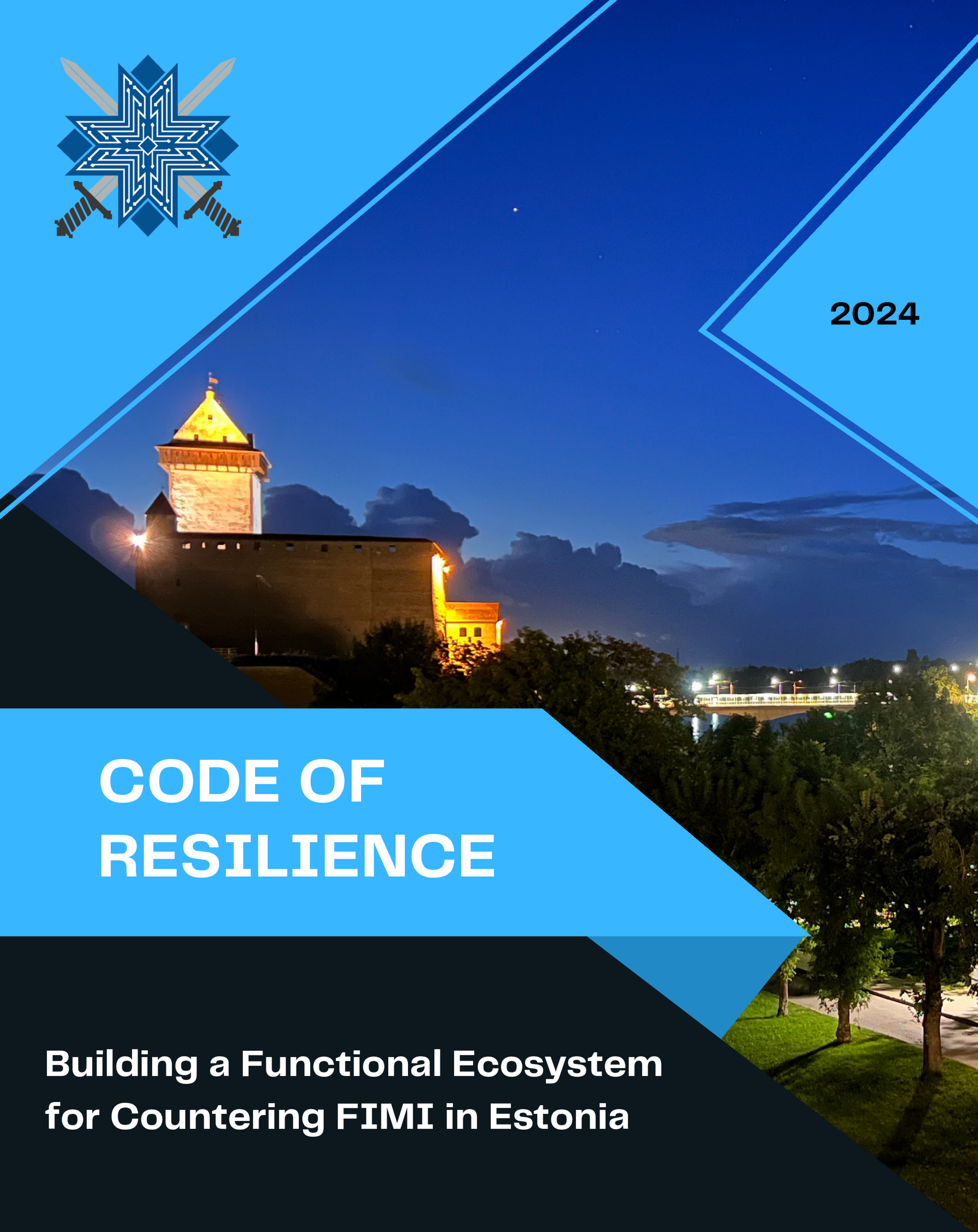

2024

CODE OF RESILIENCE

Building a Functional Ecosystem for Countering FIMI in Estonia

DMITRI TEPERIK

NATIONAL CENTRE OF
DEFENCE & SECURITY
AWARENESS

CODE OF RESILIENCE

Building a Functional Ecosystem for Countering FIMI in Estonia

Dmitri Teperik

Estonia

2024

This report has been prepared with support from IRI's Beacon Project.

The opinions expressed are solely those of the author and do not reflect those of IRI.

National Centre of Defence & Security Awareness, Estonia | kaitsen.ee

ISBN 978-9949-7355-9-4 (pdf)

Content

Executive Summary

Since the restoration of Estonian independence, Russia has persistently sought to exert malign influence in various domains on Estonia over the past three decades. Consequently, the operational agenda of Estonian policymakers has included the objective of increasing resistance to Russia's hostile disinformation since 1991. In its hostile information influence activities against Estonia, Russia has been pursuing a number of parallel objectives. These include the deepening of divisive lines within Estonian society and the compromising of Estonia's international image, particularly in relation to its status as a member of both NATO and the EU. Nevertheless, as of autumn 2024, there are no visible successes of Russian disinformation or other manipulation in or about Estonia, which gives some confidence in the effectiveness of the multilateral countermeasures and principles cultivated in recent decades to build and maintain resilience to foreign information manipulation and interference (FIMI). As set forth in the strategic documents, national security is addressed from a comprehensive perspective that encompasses cooperative interoperability between a diverse array of stakeholders and bodies, including military and civilian organisations, with the objective of effectively addressing conventional and hybrid threats, including FIMI.

An adaptive learning mindset should be encouraged and promoted among various groups of resilience stakeholders (including politicians, government officials, law enforcement agencies, municipal authorities, local communities, libraries, museums, schools, NGOs etc) in Estonia, whose vulnerability to FIMI may increase in the coming years due to technological advancement of potential adversaries on the one hand, and intellectual laziness of targeted groups on the other. Given the relatively good success of the Estonian ecosystem, its resilience development motto should emphasise that what brought us here will not take us further.

Politicians in both the national and European parliaments have the power to direct resources to strengthen working counter-measures against FIMI and to prepare the systemic approach for future challenges. Furthermore, it is recommended that additional actions be taken by the Estonian Parliament (Riigikogu) to enhance further county's resilience against FIMI.

- To debate within the Riigikogu's Cultural Affairs Committee the increasing necessity for an appropriate system of knowledge and research security in Estonia's higher education institutions and research establishments, with the aim of enhancing awareness of FIMI activities in academia and implementing more effective countermeasures in collaboration with policymakers, researchers and teaching staff.
- In order to prevent the leakage of sensitive data due to human factors, the Anti-Corruption Select Committee of the Riigikogu can spearhead efforts to educate members of parliament on the potential use of elicitation techniques for the purpose of data collection or political lobbying, thereby enhancing their ability to recognise and mitigate such risks.
- The Foreign Affairs Committee of the Riigikogu can instigate a discussion on the potential risks and other implications associated with externally funded foreign visits by politicians to non-democratic countries, where they may be vulnerable to various forms of influence and psychological manipulation.
- The National Defence Committee of the Riigikogu may initiate a collaborative foresight study on prospective FIMI challenges in conjunction with leading think tanks and experts. This study would aim to elucidate the potential implications of legislative changes on future scenarios, including AI regulations and issues of cognitive warfare.
- The Constitutional Committee of the Riigikogu is empowered to propose further measures aimed at enhancing transparency requirements for the integrity of elections. These may include a mandate that all political advertisements and online content with political or influence motives clearly disclose their sources, including any foreign affiliations.
- Furthermore, the Parliament may consider the establishment of robust safeguards and incentives for whistleblowers who reveal politically and/or ideologically motivated foreign interference or manipulation activities. Such measures could encourage more insider disclosures and prevent cover-ups by ensuring that those who come forward are protected and rewarded.

Introduction

The primary focus of countering FIMI in Estonia for several decades has been on Russia's hostile activities. However, another significant actor, China, has recently also intensified its interference in Estonia's affairs.[1] While Estonia's relations with China were historically rather pragmatically calm, the Russian state has been pursuing an opportunistically aggressive strategy against Estonia for decades. This strategy exploits a range of contexts, including historic, socio-political, economic and ethno-linguistic factors, with the aim of advancing the Russian government's attempts to project information influence and spread hostile narratives within Estonian society. This has involved targeting the Estonia's weakest points and vulnerable groups with disinformation campaigns that have been orchestrated and/or inspired by pro-Kremlin forces. As the exercise of Russia's 'soft power' has been extensively researched and documented, it has been both traceable and observable since the restoration of Estonia's independence in 1991 in numerous domains, including the economy, public diplomacy, political life and culture.[2] One of the most prominent instances of a hybrid conflict is the Bronze Soldier Crisis, which also encompassed extensive cyber-attacks and disinformation operations. This crisis was orchestrated and executed by Russia in Estonia in 2007.[3]

Later, Russia's ideological confrontation with the democratic West in general, and its military aggression against Georgia in 2008 and Ukraine in 2014–2024 in particular, introduced further complexities to the multifaceted situation of disinformation and propaganda. In Estonia, these issues have been perceived and analysed through the lens of security, given the country's continued status as a target society within Russia's sphere of interest.

[1] https://cepa.org/comprehensive-reports/chinese-influence-in-estonia
https://news.postimees.ee/6769895/trojan-panda-the-heavy-hand-of-chinese-soft-power
https://doi.org/10.25143/China-in-the-Baltic-States_2022_ISBN_9789934618154_06-31
https://sinopsis.cz/wp-content/uploads/2023/08/ccpestonia0.pdf
[2] https://dspace.cuni.cz/bitstream/handle/20.500.11956/108679/120324657.pdf
https://icds.ee/en/how-to-address-the-humanitarian-dimension-of-russian-foreign-policy-2
www.academia.edu/9797494/Tools_of_Destabilization_Russian_Soft_Power_and_Non_military_Influence_in_the_Baltic_States
[3] https://icds.ee/en/the-bronze-soldier-crisis-of-2007

Russia’s Information Hostility

The Kremlin toolbox of influence has encompassed a variety of methods based on Russia's leverages and Estonia's vulnerabilities. These include the exploration of political and economic tools, an increase in energy dependence, the shaping of the worldview and attitudes of the local Russian-speaking population, the enhancement of compatriot policy, the weaponisation of history, an increase in ideological tensions, the promotion of the role of the Russian Orthodox Church, the implementation of soft power through cooperation in education and culture, the conducting of disinformation campaigns, espionage activities, the execution of cyber-attacks, and more.[4] Russia has employed information warfare tactics to advance a series of narratives that are inherently hostile in nature. These malign narratives can be broadly classified into the following categories:

1. The assertion that Estonia violates human rights due to its Russophobic regime and the presence of fascism in Estonia;
2. The claim that Estonia's economy is highly fragile and that the country is plagued by poor governance;
3. The proposition that Estonia is wholly reliant on foreign policy directives from Brussels and Washington;
4. The contention that Estonia impedes Europe's ability to benefit from amicable collaboration with Russia;
5. The allegation that NATO renders Estonia a more hazardous environment by embroiling the country in direct confrontation with Russia.[5]

[4] https://icds.ee/wp-content/uploads/2015/Henrik_Praks_-_Deterring_and_Defeating_Russia_s_Ways_of_Warfare_in_the_Baltics.pdf
https://icds.ee/wp-content/uploads/2019/12/ICDS_EFPI_Report_The_Russian_Orthodox_Church_Sherr_Kullamaa_December_2019.pdf
https://icds.ee/en/disinformation-russias-old-but-effective-weapon-of-influence

[5] www.researchgate.net/publication/360861802_Baltic_states_in_the_Russian_online_media_Monitoring_and_Analysis_of_Russian_information_space_in_May-December_2021
www.researchgate.net/publication/361396571_Russian_information_warfare_in_Estonia_and_Estonian_countermeasures
https://link.springer.com/chapter/10.1007/978-3-030-73955-3_20

The variation and combination of the above false narratives have been disseminated through a variety of media outlets, including Russian state-controlled channels, social media platforms, proxy information channels that are ideologically aligned with the Kremlin, and various agents of informational influence.[6]

Legal Framework

Although academic and expert debates on FIMI and respective countermeasures were active in Estonia before and after 2007, no consolidated national policies on the issue were in place until 2010, when the Parliament (Riigikogu) adopted a new version of Estonia's National Security Concept.[7] The strategic document replaced the previous version of 2004 and introduced several novelties, including the concept of psychological defence to counter FIMI in Estonia. The subsequent iteration of the National Security Concept was endorsed by the Riigikogu in 2017. It addressed the security environment, while delineating the policy frameworks of national diplomacy, military defence, the protection of the constitutional order and law enforcement, conflict prevention, and crisis management. Furthermore, it described the specifics of economic security and the requisite infrastructure, cybersecurity, the protection of individuals, resilience, and the cohesion of society. The document stressed the importance of a holistic – whole-of-society approach, provided explicit definitions of strategic communication and psychological defence, and emphasised the importance of generating reliable information and general awareness with the aim of strengthening national resilience.[8] The latest edition of this framework document was adopted by the Riigikogu in 2023 – as the security environment and Estonia's security capabilities evolve, the National Security Concept may be amended or supplemented

[6] https://icds.ee/en/estonias-virtual-russian-world-the-influence-of-russian-media-on-estonias-russian-speakers
www.marshallcenter.org/sites/default/files/files/2020-09/pC_v7%20Special%20Edition_en-6_Cotter.pdf
https://stratcomcoe.org/cuploads/pfiles/ncdsa-natostratcomcoe-study-3b-rus-socmedia-web-final-1.pdf

[7] www.riigiteataja.ee/aktilisa/0000/1331/4462/13316508.pdf

[8] www.riigiteataja.ee/aktilisa/3060/6201/7002/395XIII_RK_o_Lisa.pdf

to guide the preparation of sectoral development and action plans, including in the area of countering FIMI.[9]

Over the past few decades, there has been a notable advancement in institutional capabilities and the comprehensiveness of legal frameworks pertaining to the detection, prevention, and disruption of informational threats and vulnerabilities in Estonia. The mitigation of risks and minimisation of threats posed by FIMI are achieved through the implementation of strategic communication and psychological defence measures. These are designed to enhance strategic communication, strengthen societal cohesion and reinforce the positive international image of the country, while also consolidating psychological defence to neutralise hostile information attacks. The Estonian National Security Concept defines psychological defence as a multifaceted approach to disseminating information and raising awareness about activities that may seek to undermine the constitutional order, societal values, and virtues of Estonia.

The National Security Concept serves as the foundation for subsequent strategic documents in various sectors of executive governance, including the National Defence Development Plan, the Foreign Policy Development Plan, the Development Plan for Coherent Estonia, the Domestic Security Development Plan, the Cybersecurity Strategy, and other documents adopted by the government of Estonia, its ministries, and specialised agencies to address counter-FIMI measures within their respective areas of responsibility.

Planning Anti-FIMI Measures

Estonia's National Defence Development Plan contains a whole chapter dedicated to strategic communication to provide the impetus for countering FIMI in Estonia.[10] The plan delineates the realistic development objectives for Estonia's defence until 2031 (in

[9] https://kaitseministeerium.ee/sites/default/files/eesti_julgeolekupoliitika_alused_est_22.02.pdf
[10] https://riigikantselei.ee/media/1451/download

practice, the document is reviewed every four years) and is comprised of both publicly available and classified parts, the latter of which contains more detailed information regarding specific activities. Additionally, the plan enumerates the principal systematic elements of strategic communication, including situational awareness of the information environment, enhanced societal resilience, and capacities for crisis communication.

With regard to FIMI countermeasures, the Plan provides guidance on the development of rapid detection and prevention measures, as well as proactive initiatives to enhance individuals' awareness and resilience to influence activities. In order to achieve this, it is essential to enhance the media literacy of the general public, to provide training for officials, and to expand the number of professionals with the requisite expertise. Particular consideration is given to the involvement of citizens with a non-Estonian ethnolinguistic background, with the plan directing the necessity to increase their engagement with Estonian state and to ensure the dissemination of accurate information among their communities within the country. Furthermore, it is imperative to ensure the accessibility of information for individuals with diverse disabilities and other vulnerable groups. Furthermore, the Plan acknowledges the necessity for Estonia to possess the capacity to plan and disseminate messages within the global information landscape. This encompasses the ability to set agendas, adapt timings, create materials and produce content.

The Plan asserts the necessity for the integration of media and information literacy into the Estonian education system and lifelong learning programmes for adult and elderly populations. Furthermore, it is recommended that larger audiences of experts, academics, teachers, and grassroots activists be included in training programs on information attacks, societal resilience, and media literacy. The Plan identifies the primary objective of crisis communication as the dissemination of information to the Estonian population and allied nations regarding developments within Estonia, with the aim of preventing undue alarm. Furthermore, the document emphasises the importance of verifying information from reliable sources and official channels of communication. Furthermore, it is of great importance to ensure the continued accessibility of free media, the maintenance of domestic cross-agency collaboration, and the operational continuity of foreign expert networks belonging to partners and allies.

In the context of media and information literacy, it is pertinent to cite the following strategic documents, which provide a framework for the general development of the field: Estonia's Digital Agenda 2030 and Estonia's Education Development Plan 2021-2035.[11] According to the vision of the Digital Agenda 2030, Estonia should be driven by strong digital innovation and a digitally oriented mindset. This includes the skills and knowledge for a digital society to use various digital solutions in the public sector and the development of electronic communication, i.e. connectivity and the development of national cybersecurity. As far as the formal education system is concerned, media and information literacy is recognised as a cross-curricular issue to be developed in schools and universities.

Major Stakeholders of Counter-FIMI System

Historically, the neutralisation of Russia's hostile activities was not regarded as a central tenet of broader national security, but rather as a matter for closed professional military and counterintelligence circles.[12] Later, this perception underwent a transformation as the number of participating security stakeholders increased. At the legislative level, the parliamentary committee on national defence is the principal body responsible for shaping the development of Estonia's security policy. Furthermore, the two other committees within the Riigikogu, namely the Constitutional Committee and the Legal Affairs Committee, have also addressed issues related to FIMI, particularly with regard to the protection of personal data, general administrative law, and civil and penal law.

[11] https://mkm.ee/digiriik-ja-uhenduvus/digiuhiskonna-arengukava-2030
www.hm.ee/sites/default/files/1._haridusvaldkonna_arengukava_2035_kinnitatud_11.11.21.pdf
[12] www.redalyc.org/journal/5525/552565288004/html

The role of institutions in ensuring state and public security is to define the functional responsibilities of the stakeholders and to assign tasks accordingly. With regard to state institutions, the respective activities are coordinated across the Estonian Government's ministries and agencies through the National Security and Defence Coordination Unit at the Government Office of Estonia. The unit provides the Prime Minister with advice on matters pertaining to national security and defence, and oversees the management of these matters. Additionally, the State Incident Situations Centre was established at the Government Office to raise the situational awareness of the government and the strategic leaders of the state. The State Incident Situations Centre monitors developments relevant to national security and crises to provide an operational overview of international and domestic events.

Furthermore, the Government Office of Estonia assumed the role of primary coordinator for the country's responses to FIMI. The Ministry of Foreign Affairs, the Ministry of Defence, the Ministry of Justice, the Ministry of Economic Affairs and Communications, the Ministry of Culture, the Ministry of Education and Research, the Ministry of the Interior, the Estonian Police and Border Guard, the Rescue Board[13], the Defence Forces, and national security institutions collectively constitute the principal contributors to this endeavour. The same organisations disseminate information to the Estonian population regarding the most sophisticated and imminent threats to informational and psychological security.[14] As previously stated, all relevant agencies are engaged in the implementation of countermeasures against FIMI. Attaining the desired outcome is challenging for each institution in isolation; therefore, it has been determined that the advancement of the sector will be spearheaded and orchestrated by the Government Office. Each ministry and state agency in Estonia has at least one official who has undergone training in and is tasked with specific responsibilities pertaining to strategic communication within the purview of that organisation. Coordination meetings are held on a weekly basis, while comprehensive reporting

[13] The Estonian Rescue Board is the lead agency for civil protection, responsible for sheltering, large-scale evacuation, hazard notification and improving people's preparedness for crises. It is also responsible for developing the crisis preparedness of local authorities and their communities.

[14] www.riigikantselei.ee/en/supporting-government-and-prime-minister/organisation-and-planning-work-government/national
www.riigikantselei.ee/en/strategic-communication

events are convened annually and involve a larger number of stakeholder representatives, including domestic and international partners.

In addition to its military functions, the Estonian Ministry of Defence plays a pivotal role in fostering and reinforcing the connection between citizens and the state through a range of activities. The Estonian Ministry of Defence and the General Staff of the Estonian Defence Forces have traditionally been home to one of the most advanced teams of experts on strategic communications. This is largely due to their professional activities, which have been planned and executed in response to Russia's information warfare on Estonia.

The publicly available annual reports of the Estonian Foreign Intelligence Service and Estonian Internal Security Service provide a comprehensive overview of the countermeasures employed by the Estonian government to protect its national interests from the geopolitical, economic, societal and cultural influence of foreign actors, primarily Russia and China. Additionally, the reports detail the security threats that have emerged from or are linked to Russia and other authoritarian regimes.[15] The Information System Authority of Estonia publishes an annual Cyber Security Assessment report, the objective of which is to inform both decision-makers and the general public about digital threats and other FIMI activities in the cyber domain.[16].

Two mutually reinforcing platforms were established with the objective of facilitating constructive involvement of additional non-state stakeholders (e.g. civil society, civilian experts, and private businesses) in the coordination and implementation of various activities to counter FIMI threats and attacks on Estonia. The Estonian Defence League's Cyber Unit, which was established in 2008, is a voluntary organisation whose purpose is to protect Estonian cyberspace. The principal aims of the platform are the protection of Estonia's digital lifestyle and advanced technological infrastructure, in addition to the promotion of collaborative initiatives between public and private entities

[15] Annual reviews of the Estonian Internal Security Service, https://kapo.ee/en/content/annual-reviews
Annual reviews of the Estonian Foreign Intelligence Service, www.valisluureamet.ee/assessment.html

[16] The Information System Authority is a separate agency which acts as the National Cyber Security Centre of Estonia and coordinates the development and administration of information systems ensuring the interoperability of the state's information system, organises activities related to information security, and handles security incidents in Estonian computer networks. Information System Authority is within the administrative area of the Ministry of Economic Affairs and Communications. https://ria.ee/en/authority-news-and-contact/news-media-contact/studies-analyses-overviews

in the safeguarding of IT systems within the country. The platform comprises experts occupying pivotal roles in the domain of cybersecurity within the context of critical national infrastructure, as well as individuals espousing a sense of national pride and possessing IT proficiency, including younger members of the population who are willing to contribute to the advancement of cybersecurity. Furthermore, the platform includes professionals from diverse fields who possess expertise in areas pertinent to cybersecurity, such as legal and economic expertise.[17] Frequently designated the Estonian Cyber Defence League, this platform represents an innovative model for the engagement of volunteers in national cyber defence, with due consideration of the legal context pertaining to the utilisation of volunteers in the aforementioned activities.[18]

Another illustrative example of a cooperative platform is a communications reserve, also on a voluntary basis, which brings together specialists from various fields (media, strategic communications, public relations, advertising, etc.) to support the Estonian authorities in their crisis communications, including the countermeasures of FIMI.[19] In Estonia, strategic communication is regarded as a means of reinforcing societal cohesion, with the objective of addressing security concerns through a community-based strategy that engages civil society networks and volunteers. This approach enhances societal resilience and strengthens deterrence against FIMI.[20]

Timeline of Evolving Approach

The following timeline provides a brief non-exhaustive overview of the actions and decisions taken by the Riigikogu and the Government to develop a systematic approach to countering FIMI in Estonia.

[17] https://www.kaitseliit.ee/en/cyber-unit

[18] https://ccdcoe.org/library/publications/the-cyber-defence-unit-of-the-estonian-defence-league-legal-policy-and-organisational-analysis

[19] https://digiriiul.sisekaitse.ee/bitstream/handle/123456789/2699/2021%2001%20personalireserv-WEB.PDF

[20] https://liia.lv/en/publications/societal-security-in-the-baltic-sea-region-expertise-mapping-and-raising-policy-relevance-716

2008	The adaptation of the Cyber Defence Strategy 2008-2013 reflects the lessons learned from the major cyberattacks of 2017. It was the first national strategy document to recognise the interdisciplinary nature of cybersecurity and the need for coordinated actions against FIMI in the digital domain.[21]
2010	Adaptation of the National Security Concept, where the term of psychological defence against FIMI was introduced in the legislation.[22]
2010	Adaptation of the National Defence Strategy that addresses the identification of hostile influences and the implementation of protective measures.[23]
2014	An unsuccessful attempt to establish the Problems Committee of the Riigikogu with the objective of examining the malign influence of the Russian Federation TV channels in Estonia.[24]
2017	Revision of the National Security Concept by the Riigikogu. The development of comprehensive countermeasures against FIMI is part of the strategic actions.[25]
2018	Adaptation of the Cyber Security Act and the Cyber Security Strategy 2019–2022 to achieve the strategic goals of maintaining a sustainable digital society in Estonia, supporting the cybersecurity industry, research and development, being an international leader and raising awareness of a cyber-literate society.[26]
2021	The National Defence Committee of the Riigikogu initiated a public discussion on the challenges facing national defence, which was identified as a matter of significant national importance.[27]
2022	The Legal Affairs Committee initiated amendments to the Penal Code to prohibit the use of symbols supporting acts of aggression (including

[21] www.riigiteataja.ee/akt/12960860

[22] www.riigiteataja.ee/akt/13314462

[23] https://kaitseministeerium.ee/sites/default/files/elfinder/article_files/riigikaitse_strateegia_2010.pdf

[24] www.riigikogu.ee/tegevus/eelnoud/eelnou/79c2c312-5350-4009-a8e7-331918eb3e9b/riigikogu-otsus-riigikogu-probleemkomisjoni-moodustamine-vene-foderatsiooni-telekanalite-mojutustegevuse-vastustamiseks

[25] www.riigiteataja.ee/aktilisa/3060/6201/7002/395XIII_RK_o_Lisa.pdf

[26] www.riigiteataja.ee/en/eli/ee/523052018003/consolide/current

[27] www.riigikogu.ee/en/sitting-reviews/the-riigikogu-discussed-the-development-of-national-military-defence-as-a-matter-of-significant-national-importance

	genocide, a crime against humanity or a war crime) by foreign states, as enacted by the Riigikogu.[28]
2023	The National Defence Committee of the Riigikogu discussed the importance of psychological defence against FIMI.[29]
2023	Revision of the National Security Concept by the Riigikogu. The newest version of the strategic document re-enforces the importance of countering the asymmetric means, such as information influence activities, energy dependency, engineered migration or destabilising activities in cyberspace.[30]
2024	The Constitutional Committee of the Riigikogu initiated the statement to declare the Moscow Patriarchate an institution that supports Russia's military aggression. The parliament adopted the declaration with 75 out of 101 members voting in favour.[31]
2024	Based on the Parliament's decision, the Estonian Ministry of the Interior has initiated an official investigation into potential solutions to the issue of the Russian Orthodox Church in Estonia.[32]
2024	Estonian state authorities name Russia's military intelligence in a first-ever attribution of cyberattacks.[33]

Key Requirements for and Challenges to Information Resilience

The experience of Estonia demonstrates that three factors are indispensable for resilience against FIMI. Firstly, there must be the formulation and implementation of

[28] www.riigikogu.ee/en/press-releases/plenary-assembly/the-riigikogu-banned-using-of-symbols-supporting-acts-of-aggression-by-foreign-states

[29] www.riigikogu.ee/pressiteated/riigikaitsekomisjon-et-et/riigikaitsekomisjon-psuhholoogilise-kaitse-tahtsust-ei-tohi-alahinnata

[30] https://dhs.riigikantselei.ee/avalikteave.nsf/documents/NT003B6B36/$file/Eesti%20julgeolekupoliitika%20alused_eng_22.02.2023.pdf

[31] www.riigikogu.ee/en/news-from-committees/constitutional-committee/riigikogu-declared-the-moscow-patriarchate-an-institution-sponsoring-russias-military-aggression

[32] https://siseministeerium.ee/en/declaring-moscow-patriarchate-institution-supporting-military-aggression

[33] https://vm.ee/en/news/estonia-names-russias-military-intelligence-first-ever-attribution-cyberattacks

strategic communications in accordance with a robust national framework of structural documents. Secondly, an environment must be created that safeguards the autonomy of the media. Thirdly, public confidence in democratic processes and state institutions must be preserved.

In Estonia, there is a consensus among politicians and a general awareness among the population of the potential dangers posed by FIMI to the country. As of the summer of 2024, 94% of Estonians identified disinformation as one of the most significant threats to global peace and security. Furthermore, the dissemination of fake news was identified as the most significant potential security threats to Estonia, with 86% of respondents citing them as a primary concern. This was followed by cyberattacks (84%) and foreign interference in Estonia's political and economic affairs (64%).[34]

In general, the Estonian population tends to have a strongly positive attitude of participatory democracy. In Spring 2024, 54% of Estonians were satisfied with how democracy works in the country, while general support for democracy, as a system based on equality, human rights and freedoms, and rule of law, was 84%.[35] The vast majority of respondents (89%) indicated that a sense of belonging to Estonian society was a significant factor in their lives.[36] A majority of Estonians expressed confidence in the president (74%), the judicial system (72%) and local authorities in their communities (65%), while national government was trusted by 43% of the respondents.[37] As instrumentalization of values through trust is an important indicative mechanism, the resilience of democratic political systems, including electoral processes, institutions and citizenry, makes them less vulnerable to FIMI of illiberal and authoritarian challenges.[38] Sharing and practising democratic values through strong judicial constraints and strong institutions is therefore a very important prerequisite for resilience against FIMI.[39]

[34] www.kaitseministeerium.ee/sites/default/files/avalik_arvamus_ja_riigikaitse_mai_2024.pdf
[35] www.globsec.org/sites/default/files/2024-05/GLOBSEC%20TRENDS%202024.pdf
[36] www.riigikantselei.ee/sites/default/files/documents/2024-07/2024%2006%20AA%2019%20seire%20raport%20_avaldamiseks.pdf
[37] www.kaitseministeerium.ee/sites/default/files/avalik_arvamus_ja_riigikaitse_mai_2024.pdf
[38] Merkel, W., & Lührmann, A. *Resilience of Democracies: Responses to illiberal and authoritarian challenges, Democratization*, 28:5, 869-884, 2021, https://doi.org/10.1080/13510347.2021.1928081.
[39] Boese, Vanessa, A., et al. *How democracies prevail: democratic resilience as a two-stage process. Democratization, Vol. 28*, 5 885-907, 27 Apr. 2021, https://doi.org/10.1080/13510347.2021.1891413.

Free access to information creates wider possibilities for citizens' situational awareness, and thereby contributes to a stronger resilience at the personal and societal levels.[40]. The Estonian media landscape is considered to be mature enough to ensure political independence of and wide pluralism among the media outlets.[41] With a score of 86.44, Estonia ranks 6 out of 180 countries in the 2024 World Press Freedom Index.[42] As of spring 2024, 65% of Estonians considered the media in the country to be free.[43] As indicated by the 2023 Media Literacy Index, Estonia occupies the 4th position among 41 European countries. It is situated within a cluster of countries that demonstrate the greatest resilience to the detrimental effects of FIMI, largely due to the efficacy of its educational system, the autonomy of its media, and the high level of trust among its citizens.[44]

Nevertheless, certain issues have the potential to polarise Estonian society, thereby providing opportunities for malevolent actors to undermine the country's stability. In addition to concerns regarding the significant economic underperformance, perceptions of wellbeing are intertwined with geopolitical agendas, including support for Ukraine and migration.[45] Moreover, an ethnolinguistic divide exists in Estonia, whereby the threat perceptions, level of trust and worldview of some non-Estonians diverge from those of the majority of Estonians.[46] As of the summer of 2024, 59% of respondents expressed opposition to the proposal of augmenting the legal immigration of foreign nationals to enhance Estonia's competitiveness by attracting a labour force from abroad. Only 29% of respondents in Estonia confirmed that they had a plan in place in the event of a major crisis (e.g. changes to daily living arrangements and coping mechanisms), suggesting that there is room for improvement in practical resilience, while 33% believed that their municipality or local community could effectively manage

[40] https://icds.ee/en/why-does-resilience-need-a-telescope-to-prevent-disinformation
Burnside-Lawry, J. and Carvalho, L., *A stakeholder approach to building community resilience: Awareness to implementation, International Journal of Disaster Resilience in the Built Environment, Vol. 7*, No. 1, pp. 4-25, 2016. https://doi.org/10.1108/IJDRBE-07-2013-0028.

[41] www.kul.ee/media/266/download
www.researchgate.net/publication/346653945_Eesti_meediamaastik_kumne_aasta_parast_neli_voimalikku_arengustsenaariumi

[42] https://rsf.org/en/index

[43] www.globsec.org/sites/default/files/2024-05/GLOBSEC%20TRENDS%202024.pdf

[44] https://osis.bg/wp-content/uploads/2023/06/MLI-report-in-English-22.06.pdf

[45] www.strategeast.org/all_reports/Westernization-Report-2024.pdf

[46] https://icds.ee/en/the-glass-of-societal-resilience-half-empty-or-half-full-perceptions-of-socio-economic-threats-and-wellbeing-in-estonia

a potential crisis. Regarding support for Ukraine, 48% of respondents agreed that Estonia should not rule out any way of supporting Ukraine militarily, while 41% disagreed. In addition, 59% were in favour of sanctions against Russia (while 35% were against), even if it meant a significant increase in energy and food prices. In addition to global concerns, the public's attention in Estonia was largely focused on the economic challenges posed by stagnation, high inflation, and rising taxes, which collectively overshadowed the ongoing war in Ukraine.[47]

Conclusions and Recommendations

Estonia's experience is considered one of the most successful examples of systematic approaches to mitigating the risks of foreign influence and information disruption, as the country has developed a legal framework of strategic documents, as well as various instruments and models of public-private partnerships and cooperation in building information resilience, designed to be complementary, scalable, affordable and credible.[48]

Recognising the importance of long-term partnerships, Estonia is developing and promoting multi-level cooperation (political leaders, officials, managers, operators, analysts) between NGOs, state institutions and the media to build trust in communication and knowledge sharing. In addition, Estonia is supporting local companies to develop tools for better situational awareness in the information space to increase societal resilience across the public and private sectors. The partnership also involves Estonian universities and academic research communities. Consequently, the multi-stakeholder model of security in Estonia frames approaches

[47] www.riigikantselei.ee/sites/default/files/documents/2024-07/2024.06_avaliku%20arvamuse%20uuringu%20raport.pdf

[48] https://icds.ee/wp-content/uploads/dlm_uploads/2022/10/ICDS_Report_Resilience_Against_Disinformation_Teperik_et_al_October_2022.pdf
www.bbc.com/future/article/20220128-the-country-inoculating-against-disinformation
https://cepa.org/the-evolution-of-russian-hybrid-warfare-estonia
www.csis.org/blogs/post-soviet-post/countering-russian-disinformation

to resilience against FIMI. This model divides clear responsibilities between public (state and civil society) and private (business) stakeholders directly involved in building preparedness and implementing countermeasures against disinformation, and promotes the idea of shared ownership of resilience.

The promotion of national security-related values and virtues in society is regularly carried out by political leaders and active citizens at different levels and on different platforms. These formats include peer-to-peer meetings, formal education and informal training, all embedded in local events and everyday life as a community-based approach, maintaining a tangible presence on social media and recognising active volunteers in various fields. Such activities encourage all members of civil society to contribute to strengthening national resilience. Furthermore, Estonia has been implementing select foreign experiences, including those derived from the EU and NATO, thereby also deriving benefits from the cross-fertilisation of ideas in international cooperation to counteract FIMI in various domains.

A diverse ecosystem and continuous symbiosis between state institutions, the private sector and civil society should be promoted and financially supported as a key element of national resilience. Its strengthening is based on eliminating obvious internal and external vulnerabilities, providing decision-makers with qualitative and quantitative situational awareness, and adequately informing the general public about current threat assessments and preparations in order to minimise the harmful effects of FIMI against Estonia. More useful development characteristics can be drawn from the BEACON model for building resilience in the Baltic states.[49]

In light of the challenging circumstances currently facing Estonia's economic outlook, coupled with the evolving nature of geopolitical hybrid threats, it is imperative that the appropriate level of investments is maintained in order to ensure the full functionality of the ecosystem for countering FIMI. This entails ensuring the presence of the following key elements: systemic approach, flexibility, networking, complementarity, awareness and professional commitment.

[49] www.researchgate.net/publication/374701312_The_BEACON_model_for_resilience_building_in_the_Baltics_key_lessons_to_learn_from_Ukraine

The Riigikogu has an important role to play not only in approving the state budget, but also in organising regular public hearings on potential threats from FIMI, including the growing misuse of AI, China's efforts to advance cognitive warfare, etc. The expert consultations in Parliament would help to raise awareness among politicians and state officials, as well as draw the attention of the media and the general public to the issues of FIMI.

As human beings, parliamentarians themselves can be susceptible to various manipulative psychological techniques or disinformation campaigns employed by a malevolent foreign entity or its domestic proxies, and therefore elected politicians and their political advisors need a greater awareness of FIMI threats and training to avoid elicitation during foreign visits or lobbying events.

In addition, Riigikogu members could initiate FIMI-related knowledge exchange on lessons learned and future foresight with their counterparts from other legislative bodies in Europe, including the European Parliament, as collaborative efforts can help track and counteract cross-border disinformation campaigns more effectively.

ISBN 978-9949-7355-9-4 (PDF)

NATIONAL CENTRE OF DEFENCE & SECURITY AWARENESS
ESTONIA | KAITSEN.EE