AUSTRIAN INSTITUTE FOR EUROPEAN AND SECURITY POLICY

Nr. 2025/5

# Building Societal Resilience Against Hybrid Threats

## Comparative Insights from Finland and Lithuania

by Matthias Helf and Nick Nieschalke

July 2025

AIES FOCUS

# Building Societal Resilience Against Hybrid Threats
# Comparative Insights from Finland and Lithuania

*This publication builds upon insights generated during the panel discussion "Strengthening European Security: Enhancing Societal Resilience against Hybrid Threats", held on 8 April 2025 in Vienna. The event was jointly hosted by the Austrian Institute for European and Security Policy, the Embassy of Finland in Vienna, and the Embassy of Lithuania in Vienna. We are grateful for the valuable contributions and perspectives shared by the panellists: Mr. Teemu Tammikko (Senior Research Fellow, Finnish Institute of International Affairs), Mr. Darius Domarkas (Head of the Public Security Policy Department, Ministry of the Interior of the Republic of Lithuania), and Mr. Janne Känkänen (CEO, National Emergency Supply Agency of Finland).*

## Introduction

Austrian President Alexander Van der Bellen recently described Finland as "the land of resilience," a fitting attribute to a nation shaped by its proximity and fraught history with Russia. At the heart of Europe's response to modern security challenges is the Helsinki-based European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE). Established in 2017, the Hybrid CoE serves as a vital hub for the EU and NATO, enhancing resilience and preparedness against hybrid threats such as disinformation, cyberattacks, and assaults on critical infrastructure. It functions as a key knowledge and training platform, facilitates strategic dialogue, and supports member states in developing integrated national approaches. While formally part of neither the EU nor NATO, the Hybrid CoE's work is anchored in several key EU frameworks, such as the Joint Framework on Countering Hybrid Threats (2016), the EU Security Union Strategy (2020–2025), the Strategic Compass (2022), and the Cybersecurity Strategy (2020) – all of which prioritize resilience, situational awareness, and rapid, coordinated responses.

Not only the Russian war of aggression against Ukraine, but also the sharp rise of hybrid attacks on the European Union and its member states underscores the urgent need to further strengthening Europe's collective resilience – in terms of conventional defensive capabilities, but across society.

In 2024 alone, the European Union faced some 10,000 cyber-attacks with public administration, transportation, as well as banking and finance being the primary targets[1]. Baltic countries are particularly affected: Since Russia's invasion of Ukraine, cyber-attacks in Latvia against "state institutions and critical infrastructure have quadrupled"[2]; furthermore, the Baltics have been one of the primary targets for disinformation campaigns, weaponized migration and attacks on critical infrastructure – making them first movers and role models in building up preparedness and boosting societal resilience[3]. Similarly, the recent damaging of undersea cables in the Baltic Sea serve as a stark reminder of the growing exposure of Europe's critical infrastructure to hybrid interference, and the cascading effects such disruptions can have on public confidence, cohesion, and continuity of services.

This paper aims to outline the initiatives implemented by both Finland and Lithuania, take stock of Austria's current progress in building up societal resilience and preparedness, and ultimately derive recommendations to further support and strengthen these efforts.

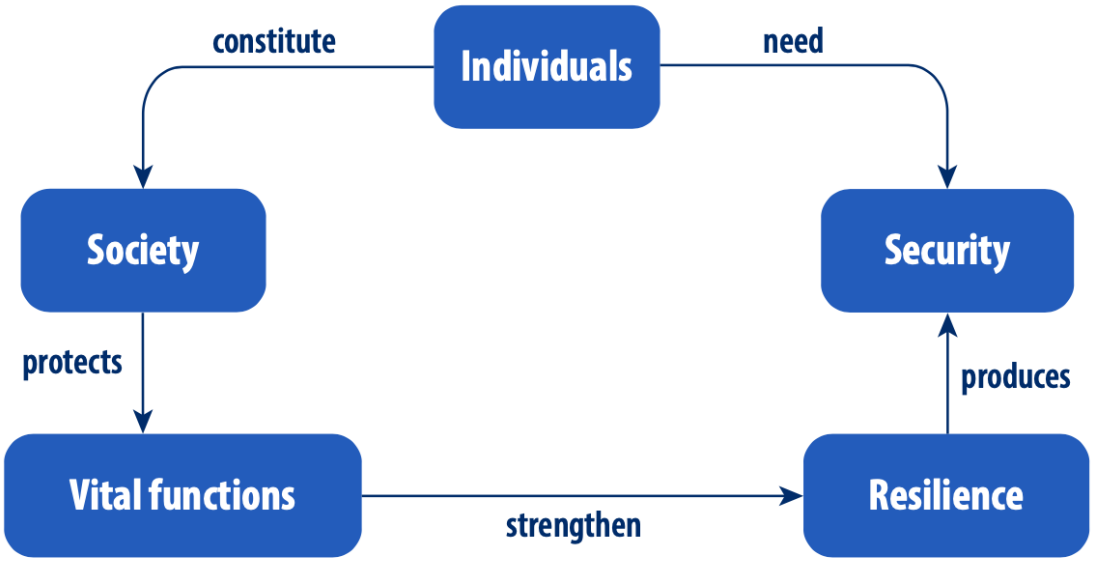


Figure 1 – Security Strategy for Society, 2025, p.13

It is emphasized that Austria, with its comprehensive national defence approach, shares a similarly broad understanding of the role of civil society in national security as Finland and Lithuania. However, differences exist in the structuring and institutionalization of cooperation among public and private actors, and civil society, in countering hybrid threats. While Finland and Lithuania explicitly assign responsibilities to civil society and individuals in building resilience, this approach is only present to a limited extent in Austria's national defence strategy. As a result, there is a divergence in threat awareness between Austrian public security actors and civil society, and consequently, a limited willingness within civil society to actively engage in countering hybrid threats or to build acceptance for corresponding defensive measures.

## Finland

Finland's strategy for social resilience against hybrid threats has its roots in the Cold War era. The Soviet Union as an immediate neighbour and the fundamentally uncertain geopolitical situation necessitated a preparedness for a variety of, even subtle, non-military attacks from abroad[4]. The comprehensive security approach, which was pursued from the outset and involved the resources of the armed forces, civil society, and importantly, both the internal security (police, customs, border guards, civil protection) and the private sector in crisis preparedness, represented an early example of integrated crisis preparedness.

Unlike in other European countries, this comprehensive approach to crisis prevention was continued even after the end of the Cold War to address evolving security challenges.[5] In the "Strategy for Securing Vital Functions for Society", published by the Finnish government in 2003, the role of society as an actor in crisis management was already prominently mentioned. Later strategy papers increasingly mention civil society in the form of individuals as well as non-governmental organizations (NGOs), and in 2010 the strategy papers were renamed "Security Strategy for Society", which emphasized the role of society in the comprehensive security model[6].

The annexation of Crimea by Russia in 2014 and the increase of Russian hybrid attacks in the Baltic states and Ukraine prompted a broader recognition of the need to adapt national security approaches to such threats. The concept of "hybrid threats" only entered the European security discourse after 2014, including in Finland, where it was deliberately framed to extend beyond a purely military context. The 2016 EU joint framework on hybrid threats set

the language and laid the groundwork for later national strategies, including Finland's.

Finland subsequently played an active role during its Council Presidency in 2019, shaping this emerging agenda at the EU level, and contributing to the establishment of the ad hoc Hybrid Working Party (HWP) in the Council, later institutionalized as the HWP on Enhancing Resilience and Countering Hybrid Threats (ERCHT)[7,8]. Finland also hosts the aforementioned Hybrid CoE in Helsinki, further underscoring its central role in European resilience building and reflecting its long-standing commitment to comprehensive security. In response to these new threats the Finnish government published the Security Strategy for Society in 2017, which understood comprehensive security as a deeply and broadly integrated social collaboration model. Thus, in addition to a comprehensive whole-of-governance approach, it also incorporated a whole-of-society approach – extending beyond state actors to include non-state actors in exercises and preventive crisis preparedness measures – while formalizing and structuring the exchange and analysis of security-relevant information between civil society and public institutions.[9]

The 2025 iteration of the Security Strategy for Society continues this trajectory, emphasizing the role of individuals and society in protecting vital functions against hybrid threats, especially in light of increased hybrid interference from Russia since the beginning of its war of aggression against Ukraine in 2022. The Security Strategy for Society 2025 emphasizes the importance of the preparedness of individuals and society to protect vital functions of Finnish society in order to build state-wide resilience against hybrid threats (Figure 1).

The following vital functions have been identified as worthy of protection[10]:

- Leadership
- International and EU activities
- Defence capability
- Internal security
- Economy, infrastructure, and security of supply
- Functional capacity of the population and services
- Psychological resilience

These vital, closely interconnected functions are assigned to actors ranging from public administration, the business community, civil society, to individuals, each having been identified as crucial stakeholders, thus bearing specific security-related responsibilities.

The close and structured cooperation between public administration and business actors exemplifies the centrality of public-private collaboration in Finland's security approach. Integrated networks between public administration and business actors allow for a common situational awareness across sectors and levels by means of a structured exchange of information on hybrid threats and can thus derive coordinated measures from this.

For example, common threats to critical infrastructures and supply chains are identified and a joint strategy for countering these can be developed. The cooperation between private and public actors is based on a binding but voluntary cooperation, which is established through legal requirements, joint exercises, obligations, and cooperation agreements. The aim of this cooperation is to establish communication between authorities and companies as quickly as possible in the event of a crisis. To give the cooperation an institutionalized structure, the National Emergency Supply Agency (NESA) was established in 1993 to serve as the secretariat for the National Board of Economic Defence (NBED) operating under the Ministry of Economic Affairs and Employment.

Although NESA's core mission remains the maintenance of supplies in the event of an emergency, twenty-three, voluntary but highly institutionalized, sector-specific NESA cooperation pools contribute to maintaining a comprehensive situational overview of the security environment and resilience capacities across sectors. Originally primarily concentrating on the supply of material goods, NESA additionally evolved into a key actor in countering hybrid threats. For example, the media pool engages media companies in efforts to safeguard continuity of communication, counter disinformation, and uphold media freedom during crises. Thus, NESA functions as an important interface between civil society,

public authorities, and companies to maintain critical services even in the event of large-scale or new types of attacks. The exchange in the twenty-three pools as well as the regular updating of NESA's strategic orientation, determined by the government and through cooperation with all social actors, also ensures that the agency is always flexibly prepared for a variety of threats.

Another exemplary feature of the Finnish strategy for countering hybrid threats is the aforementioned inclusion of civilian individuals as security actors. Skills in media literacy and digital capability are considered vital to national security[11]. Personal initiative, neighbourhood support and building trust in society are considered an important pillar of resilience building, and pursued through the involvement of individuals in countering hybrid threats[12]. The citizen is thus not only seen as requiring protection from hybrid threats, but as an active agent in building resilience with the additional goal of creating a sense of responsibility for national security[13].

In conclusion, two approaches to countering hybrid threats can be derived from the Finnish example as particularly instructive for Austria. Firstly, Finland already has a deep and broadly structured cooperation between civil society, public actors, and economic authorities. Both the Whole-of-Governance and the Whole-of-Society principles embedded in Finland's comprehensive security model enable a shared understanding of hybrid threats as challenges that concern all sectors of society. Crucially, these approaches not only ensure that potential threats are recognized early – thereby enhancing situational awareness – but also facilitate a flexible and multi-layered response across institutional boundaries.

> The citizen is thus seen ... as an active agent in building resilience.

Without such integrated frameworks, hybrid interference activities might go unnoticed or unaddressed. The ability to draw on a broad set of instruments – including diplomatic, economic, legal, and information measures – is central to an effective and appropriate response. NESA presents itself as a particularly structured and, due to its legal and social anchoring, established and yet adaptable interface authority for coordination. Another exemplary feature of the Finnish approach is the recognition of the individual as both a target and an actor in responding to hybrid threats. Joint situation and risk assessment involving civil society, as well as the systematic preparedness of citizens, foster both awareness and resilience, thus ultimately strengthening social cohesion in the face of disruption.

## Lithuania

Similarly, the Baltic states, particularly Lithuania, face hybrid threats such as disinformation, cyberattacks, social polarization, and malign foreign influence operations. Lithuania has responded by further developing comprehensive resilience strategies integrated into its national security architecture. Lithuania's total defence concept is grounded in Article 3 of the Constitution, which grants every citizen the right to resist threats to the country's independence and constitutional order. This principle was operationalized in the 1997 Law on the Foundations of National Security, which introduced the idea of universal and unconditional defence, assigning responsibilities to both the state and its citizens to prepare for civilian resistance in case of aggression.

More precise developments have emerged in recent years. The 2021 National Security Strategy broadened the scope of national defence to include not only military forces but also civil institutions, municipalities, the private sector, and – importantly – individual citizens. A review of the Strategy, initiated with the aim of reflecting the evolving security landscape, is underway and scheduled to be finalised by the end of 2025, though its underlying whole-of-society approach is expected to remain unchanged. A 2022 strategy on civil resistance further emphasized that total defence encompasses both armed and non-armed forms of defence, declaring civil

resistance a core element. Under this approach, every citizen – regardless of age – shares responsibility for preventing threats and resisting occupation, embedding national defence deeply into all levels of society[14]. As the concept positions social resilience as a central national resource, citizens are, inter alia, expected to contribute not only physically but through civic engagement and information literacy as well[15,16].

In contrast to traditional security approaches, the Lithuanian total defence approach actively addresses hybrid threats from the bottom up and relies on participatory mechanisms. In light of the rise in cyberattacks and disinformation campaigns by Russia since 2014 – intensifying further after the full-scale invasion of Ukraine in 2022 – media and digital literacy have become central pillars of Lithuania's resilience strategy. The ability to critically access, evaluate, and verify information is regarded as an essential civic duty. The development of these skills is actively promoted by both state institutions and civil society and is considered a core responsibility of the Lithuanian state[17].

Furthermore, a key element of Lithuania's societal resilience strategy is the integration of practical, community-based preparedness measures through civic institutions such as the Lithuanian Riflemen's Union. With deep historical roots and strong local anchoring, the Union serves today as an important platform for voluntary civic engagement and resilience training. Open to civilians of varying ages, its programs encompass, inter alia, survival skills, first aid, and civil protection, thus embedding preparedness into everyday life. Crucially, and thanks to its historical continuity, the union serves as a practical vehicle for mobilizing society in times of crises, whether natural disasters, hybrid attacks, or conventional warfare. A decentralized structure of local chapters guarantees fast and community-based civil response capacities in emergency situations[18].

The ability to critically access, evaluate, and verify information is regarded as an essential civic duty.

Furthermore, the launch of the LT72 app further contributed to strengthening individual and household-level preparedness. The app provides practical guidelines and steps on crisis preparedness, emergency responses and relevant information on emerging threats. After its launch in April 2025, LT72 registered 62.000 downloads within the first month[19].

In addition, Civil society initiatives such as "Debunk.eu", the "Elves" networks, the Civic Resilience Initiative (CRI), or the state education program "boost your immunity" represent state and state-supported projects for building skills to counter disinformation and actively involve civil actors in combating disinformation campaigns[20].

Furthermore, a particular focus on integrating ethnic minorities into the broader social information space serves as a safeguard against both separatism and as a means of strengthening social cohesion. Providing content in minority languages, especially Russian, and targeted participation programs help reduce susceptibility to disinformation that targets and exploits fault lines in Lithuanian society[21].

The protection of the democratic order is another key element in engaging society in countering hybrid threats as these particularly target social cohesion, trust in institutions and basic democratic values in the country – often by exploiting ethnic, linguistic, or social differences. The Lithuanian strategy counters these threats with a multi-layered approach of "layered resilience"[22] . Therefore, free, pluralistic, and legally protected media are consistently strengthened. Regulatory authorities such as the Radio and Television Commission Lithuania (RTCL) enforce standards, swiftly shut down hostile or propagandistic channels and sanction hate speech as well as war propaganda[23].

An example for the efficiency of this control body was the shutdown of all Russian TV channels after the Russian full-scale invasion of Ukraine on February 24, 2022, and the simultaneous promotion of independent Russian-language media[24]. This targeted approach and integration of minorities while avoiding parallel

information communities (especially Russian-speaking communities) and strengthening the common, democratic information space is considered a strategic goal.

Multilingual educational offers and the aforementioned fact-checking initiatives further target diverse population groups and promote the capacity to detect and respond to digital manipulation. The involvement of low-threshold citizen projects in this area motivates active participation and facilitates access.

The education of Lithuanian society to engage critically with information, combined with the active involvement of civil groups in combating disinformation, illustrates how democratic discourse can be protected without infringing on civil liberties. Anchored in a solid legal framework, this approach consistently promotes individual information literacy as a civic duty, targeted and multilingual media and political education from an early age, low-threshold and inclusive fact-checking and participation initiatives, the legally secure protection of pluralistic media, and the clearly regulated integration of all minorities into the national information space. Together, these elements form a robust democratic foundation for social self-efficacy and resilience, reinforcing democratic information processes.

Community-based structures – such as the Lithuanian Riflemen's Union – play a particularly important role in translating this framework into practice by embedding preparedness and civic engagement at the local level. The broader cooperative structure ("network of resilience"), consisting of the state, business, civil society, and citizens, thus mirrors the Finnish model of comprehensive security, framing security as a shared and society-wide responsibility.

Since 2023, this approach has been further institutionalized in Lithuania with the adoption of the new Crisis Management and Protection Law, which introduced the position of *preparedness officers* both within ministries as well as municipalities. These officers are tasked with bringing all resilience and preparedness functions into a single role, while also serving as promoters of preparedness culture within their respective institutions. Moreover, the legislation encourages communication and coordination among officers, thereby contributing to the formation of an interconnected national network of resilience.

## Austria

Austria's Comprehensive National Defence (Umfassende Landesverteidigung) approach contains three non-military aspects: Mental and Moral Defence (Geistige Landesverteidigung), Civil Defence (Zivile LV), and Economic Defence (Wirtschaftliche LV). Together these encompass vital aspects of countering hybrid threats, namely Civil Defence, Civil Protection, and Disaster Management – all of which are recognized in its most recent 2024 National Security Strategy. Indeed, this strategy as well as various recent initiatives, such as the 2025 National Crisis Security Law, indicate a priority shift towards recognizing, preparing for, and responding to hybrid threats.

In the 2025 Risk Report published by Austria's Ministry of Defence, various manifestations of hybrid threats, such as cyber-attacks and disinformation, are not only recognized as threats to Austria specifically, but are also met with proposed responses that include, among others, the integration of security awareness and resilience-building into school curricula. In that sense, parallels between Lithuania's "Total Defence", Finland's comprehensive understanding of national security, and Austria's "Comprehensive Defence" approach form a foundation for further developing efforts in Austria to build societal resilience and readiness vis-à-vis hybrid threats. Given Austria's federal structure, where competencies for education, civil protection, and crisis management are shared between the federal government and the states (Länder), the effective implementation of such measures will depend on coordinated action across action across governance levels.

However, while the conceptual framework is in place, Austria could focus on various, tangible steps in order to boost both societal resilience and response capabilities to hybrid interference.

### Establish Local Civic Resilience Structures

Austria could pilot community-based, local resilience platforms or partnerships modelled on Lithuania's Riflemen's Union but adapted to an Austrian civil context. These structures should be voluntary, non-militarized, and locally anchored – for example through local association, (volunteer) fire brigades, or other municipal networks. Their purpose would be to complement professional emergency services by fostering civic preparedness, promoting situational awareness, and strengthening local cohesion. Activities could include training in emergency routines for various incidents (e.g. blackouts, severe infrastructure disruptions) and neighbourhood support structures with a particular focus on vulnerable groups.

Importantly, embedding these efforts into locally established and trusted institutions would help contribute to broader acceptance of resilience building measures without having to rely on top-down securitization. Already existing structures such as the Austrian Zivilschutzverband could in turn profit from increased visibility.

### Further Institutionalize Whole-of-Society Awareness Measures

The proposed inclusion of security awareness and digital literacy in school curricula serves as a crucial initial step in institutionalizing awareness and resilience building measures. In this context, educational efforts could place greater emphasis on digital competence, and importantly, critical engagement with information environments. Experience from both Lithuania and Finland suggest that fostering a broad understanding of hybrid threats, including their societal and psychological dimensions, contributes not only to preparedness, but democratic cohesion overall.

Public awareness campaigns coordinated with relevant ministries and civil society organizations, could further support this effort by offering accessible guidance on individual preparedness, civic responsibility, and available support mechanisms. Ensuring that such information is available in multiple languages would also contribute to a more resilient and cohesive social fabric. While model initiatives like the LT72 app released by the Lithuanian government are currently at an early stage, such efforts warrant further observation and evaluation, as they may yield valuable insights for future comparable initiatives.

### Support Low-Threshold Participation in Counter-Disinformation Efforts

The Lithuanian case demonstrates the value of involving civil society in safeguarding the information space. Initiatives like Debunk.eu or the Elves network show how voluntary civic engagement can play a meaningful role in identifying and responding to disinformation, particularly during crises as well as before and during elections.

Keeping the sensitivity and paramount importance of a free and independent information space in mind, Austria could build on this model by encouraging partnerships between select public institutions, independent media, academic institutions, and NGOs to create comparable formats tailored to its own information environment. Examples might include reporting tools for disinformation, small-scale fact-checking networks, or community workshops hosted by educational providers. These initiatives could form part of a broader, inclusive strategy to promote democratic resilience, while aiding in rebuilding trust in media and public institutions.

### Deepen Public-Private Cooperation on Hybrid Threats

Preexisting public-private cooperation, as for example outlined in the Austrian Programme for Critical Infrastructure Protection (APCIP)[25] could serve as a stepping stone for expanding such cooperation efforts beyond providers of critical infrastructure to include other sectors relevant to hybrid resilience, such as media, logistics, and education. Regular dialogue formats and joint scenario-based exercises, similar to the sector-specific coordination pools established by NESA, could foster shared situational awareness and enable coordinated crisis response planning.

Strengthening communication pathways between public authorities and private actors before crises occur would help reduce reaction times and improve Austria's capacity to respond ef-

fectively to disruptions. Voluntary, yet formalised frameworks, supported by legal clarity and mutual obligations, can encourage sustained engagement across sectors without creating excessive administrative burdens.

In sum, Austria already possesses both a normative as well as a structural foundation for boosting resilience against hybrid threats. What remains is the development of concrete, institutionalized, and societally embedded mechanisms for implementation at both a local and a larger societal level. Drawing on Nordic-Baltic models, Austria could embrace a proactive and participatory approach to security that recognises individuals and communities as key actors in national resilience.


## About the Authors

Matthias Helf is a graduate student in the Master's program in Peace and Security Studies and Research Assistant at the Institute for Peace Research and Security Policy at the University of Hamburg (IFSH). His fields of research include Russian foreign and security policy, the reorganization of the European security architecture and international climate security.

Nick Nieschalke is a Research Fellow at the Austrian Institute for European and Security Policy (AIES). His research focuses on security and geopolitical issues in the Indo-Pacific, Europe's and Austria's relations with China, as well as strategic approaches to European China policy in the context of global great power rivalry.


1 Villafani, F. (2025): Cyber-Attacks in the EU: 10,000 in the Last Year, 19% against the Administration, Global Affairs and Strategic Studies, https://en.unav.edu/web/global-affairs/ciberataques-en-la-ue-10.000-en-el-ultimo-ano-el-19-contra-la-administracion?utm_source=chatgpt.com.

2 Latvian Public Media (2024): CERT: Latvia Sees Highest Level of Cyberattacks in Two Years, https://eng.lsm.lv/article/society/crime/15.10.2024-cert-latvia-sees-highest-level-of-cyberattacks-in-two-years.a572581/.

3 Golubeva, M. (2025): Wide Awake and Busy: The Baltics Prepare for Russian Hybrid Attacks, https://cepa.org/article/wide-awake-and-busy-the-baltics-prepare-for-russian-hybrid-attacks/

4 Fjäder, C. & Schalin J. (2024): Building resilience to hybrid threats: Best practices in the Nordics. Hybrid CoE Working Paper 31, European Centre of Excellence for Countering Hybrid Threats, Helsinki. p.7 https://www.hybridcoe.fi/publications/hybrid-coe-working-paper-31-building-resilience-to-hybrid-threats-best-practices-in-the-nordics/

5 Ibid.

6 Finnish Government/Security Committee (2025): Security Strategy for Society. Government resolution. Publications of the Finnish Government 2025:3, Helsinki. p.10. https://urn.fi/URN:ISBN:978-952-383-817-8

7 Fjäder & Shalin, 2024, p. 15

8 Tuominen, H. (2022): In Defence of Common Values: The Finnish EU Council Presidency 2019, Cooperation and Conflict 58, no. 1 (1 March 2023): pp. 23–41, https://doi.org/10.1177/00108367221077639.

9 Fjäder & Shalin, 2024, p. 15; 18

10Finnish Government/Security Committee (2025) pp.15-23

11 Finnish Government/Security Committee (2025), p.23

12 Finnish Government/Security Committee (2025), p.23: pp. 43-44

13 Fjäder & Shalin (2024) p. 15; Finnish Government/Security Committee (2025) pp. 43-44

14 Rogulis, D. (2025). Understanding Lithuania's total defence approach in the face of Russian threat through principal–agent theory. Security and Defence Quarterly, 49(1), 58–73. p.65 https://doi.org/10.35467/sdq/195805

15 Lithuanian Law on Civil Protection, Art. 6 para.1-2

16 Lithuanian Law on Civil Protection, Art. 16 para. 1-3

17 Rogulis, D. (2025). Understanding Lithuania's total defence approach in the

face of Russian threat through principal–agent theory. Security and Defence Quarterly, 49(1), 58–73. p.65 https://doi.org/10.35467/sdq/195805

18 Rogulis, D. (2025), p.65; Maliukevičius, N. (2024), p.9

19 Fire and Rescue Department under the Ministry of the Interior of the Republic of Lithuania: LT72, https://lt72.lt/?lang=en

20 Maliukevičius, N. (2024). Fortifying Democracies: Lithuania's Comprehensive Approach to Counter Disinformation and Propaganda. Policy Paper, Vilnius University, Institute of International Relations and Political Science. pp. 4-5. https://www.tspmi.vu.lt/wp-content/uploads/2024/XX/policy-paper-maliukevicius.pdf

21 Macikenaite V. (2022): Societal Resilience and Societal Ethnic Consolidation: The Case of the Baltic States. In: Andris Sprūds, Una Aleksandra Bērziņa-Čerenkova, Sintija Broka (eds.): Commonalities, Risks and Lessons for Small Democracies: Hybrid Threats in Baltics and Taiwan. Riga: Latvian Institute of International Affairs, pp. 10–23. p. 18. ISBN 978-9934-567-78-0; Maliukevičius, N. (2024) pp. 7-8

22 Maliukevičius, N. (2024

23 Maliukevičius, N. (2024). P. 7

24 Ibid.

25 'Austrian Program for Critical Infrastructure Protection (APCIP)', onlinesicherheit.at, 2024, https://www.onlinesicherheit.gv.at/Services/Initiativen-und-Angebote/Strategische-Infrastrukturen/Austrian-Program-for-Critical-Infrastructure-Protection-APCIP.html.

© Austria Institut für Europa und Sicherheitspolitik, 2025

All rights reserved. Reprinting or similar or comparable use of publications of the Austria Institute for European and Security Policy (AIES) are only permitted with prior permission. The articles published in the AIES Focus series exclusively reflect the opinions of the respective authors.

Dr. Langweg 3, 2410 Hainburg/Donau

Tel. +43 (1) 3583080

office@aies.at | www.aies.at