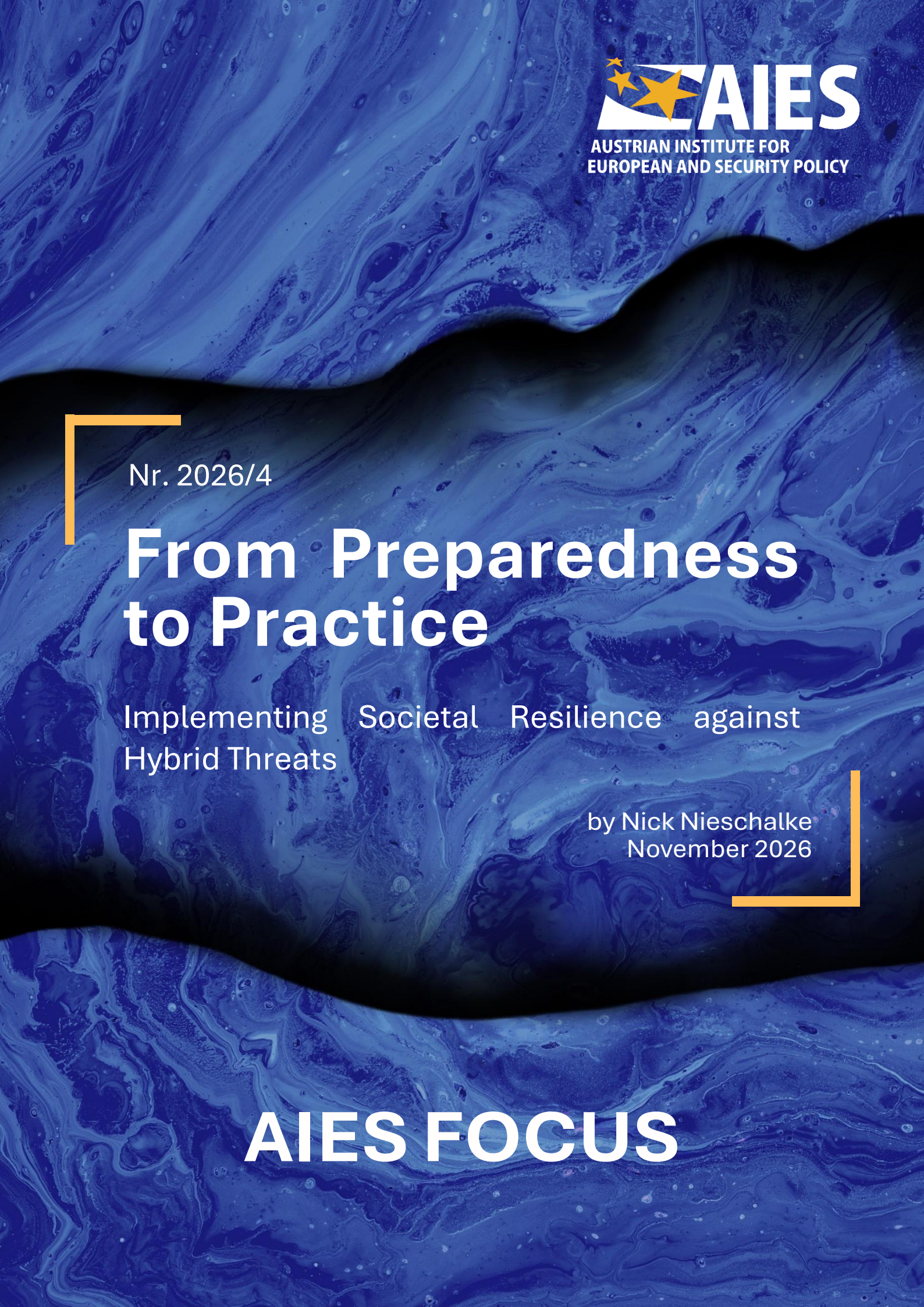

AUSTRIAN INSTITUTE FOR EUROPEAN AND SECURITY POLICY

Nr. 2026/4

From Preparedness to Practice

Implementing Societal Resilience against Hybrid Threats

by Nick Nieschalke
November 2026

AIES FOCUS

From Preparedness to Practice
Implementing Societal Resilience against Hybrid Threats

This publication builds upon insights generated during the panel discussion "From Preparedness to Practice – Implementing Societal Resilience against Hybrid Threats", which the Austrian Institute for European and Security Policy hosted in cooperation with the Embassies of Finland, Lithuania, and Poland in Vienna in June 2026. Special thanks go to the panellists for their valuable contributions and perspectives: Mr. Andreas Schlegel (Deputy Adviser to the Austrian Government on National Security, State Resilience, Comprehensive National Defence, Crisis Prevention and Crisis Management), Col (ret.) Saulius Guzevičius (Head of the International Cooperation and Information Support Division, Public Security Service, Ministry of the Interior of the Republic of Lithuania), Ms. Annukka Ylivaara (Assistant Secretary General, Security Committee, Finnish Government), and Ms. Paula Rejkiewicz (Head of the Disinformation Unit, Ministry of Foreign Affairs of the Republic of Poland).

Introduction

Over recent years, the issue of hybrid threats and attacks has moved from the periphery to the very centre of security and defence policy debates. This is primarily because, since the Russian full-scale invasion of Ukraine in early 2022, Austria and the European Union as a whole have found themselves facing an increasing number and range of hybrid attacks. In Austria specifically, with its neutrality enshrined not only in the constitution but also rooted in political tradition, the question arises as to how one should deal with this 'new normal' in practical terms. As one of the panellists pointedly remarked, neutrality is not a shield against hybrid attacks. So whilst there is still room for improvement when it comes to societal resilience and awareness vis-à-vis hybrid threats, there is a widespread recognition of those challenges on the political level, and significant progress in recent years in terms of awareness and preparedness has been made. The variety of hybrid threats ranging from the information manipulation, cyberattacks, economic coercion, drone incursions into EU territory, and all the way up to kinetic attacks, for example, on critical infrastructure demonstrates a broad arsenal of means to create a "climate of intimidation and uncertainty" (EEAS 2026). Target selection has proven equally diverse with sabotage preparations targeting military sites and critical infrastructure, but also "large retail outlets and other public places", even running the risk of fatalities (ABW 2026, p. 12).

Russia's state-media budget for 2026 alone amounts to approximately EUR 1.56 billion, representing a 7 per cent increase over 2025 (EEAS 2026). This figure is only a documented minimum since a comprehensive estimate of expenditure on cognitive warfare is not feasible, as relevant activities expectedly rely on covert funding.

In 2025, the EEAS detected 540 foreign information manipulation and interference incidents involving more than 10,500 channels. Within a mapped sample of approximately 3,000 assets, 90.5 per cent were classified as covert or non-overt. Around one quarter of detected incidents involved the use of AI tools. As with the budget case, these figures reflect detected cases and cannot be treated as representative of the overall phenomenon (EEAS 2026). Poland alone recorded almost 700,000 reports to its national Computer Security Incident Response Teams (CSIRTs) in 2025, equivalent to approximately 56,900 per month across all categories (Ministry of Digital Affairs Poland 2026, p. 10).

Finland, Lithuania and Poland each, in their distinctive ways, pursue both a whole-of-government as well as a whole-of-society approach when responding to and preparing for these challenges. In that, they assign specific roles not just to individual state institutions, but also to businesses, local governments, civil society actors and the citizens themselves. However, implementation routes do vary significantly - be it through legal, institutional or civil society vectors - highlighting the respective countries' priorities and security

models. With Austria's conceptual and institutional framework increasingly being in place, the country can draw valuable lessons from the three case studies when it comes to implementation towards civil society specifically. This Focus paper therefore primarily looks for transferable practices whilst accounting for the divergent legal traditions, institutional makeup and societal parameters between the countries in question.

Finland – Shared Responsibility

Finland approaches hybrid threats from a position of institutional continuity. Its concept of comprehensive security treats the vital functions of society as a joint task of authorities, businesses, organisations and citizens, in all circumstances and at all levels of society (Finnish Government 2025, p. 12). As was highlighted during the panel discussion, this framework operates in both "normal times and times of crises" in light of tangible threats that the country is evidently facing. Against this backdrop, the National Risk Assessment 2023, drafted by a cross-sectoral working group that included the Secretariat of the Security Committee, describes 21 threat scenarios and disruptions of national significance and lists information influence activities first (Ministry of the Interior Finland 2023, pp. 11, 31-91.). It is worth noting that the National Risk Assessment will expectedly be updated by the end of 2026 (Ministry of the Interior of Finland 2026).

In turn, the central implementation instrument is the Security Strategy for Society, adopted as a government resolution in January 2025 and the fifth version since 2003 (Finnish Government 2025, p. 10). It breaks the seven vital functions down into 56 strategic tasks, each assigned to responsible ministries. Each task in turn has one designated lead ministry responsible for coordinating it and compiling the reporting (Finnish Government 2025, pp. 29, 47). This visibility of responsibility prior to a crisis occurring reduces or even preempts the need to improvise coordination in high-pressure scenarios ensuring high levels of preparedness and resulting responsiveness.

Notably, only two of these tasks are explicitly militarily connected (Finnish Government 2025, p. 47) with the other 54 belonging to the civil domain underscoring yet again how civilian actors crucially contribute to the shared responsibility of societal preparedness. At the same time, the tasks themselves rest on legislation, are formalised through agreements and are complemented by voluntary activities drawing in the wider society (Finnish Government 2025, p. 12). Concretely, businesses own and operate most critical functions and are thus subject to legal continuity requirements, municipalities are bound to contingency planning, and civil society organisations (e.g. the Finnish Red Cross) coordinate volunteers and feed into situational awareness (Finnish Government 2025, pp. 41–42). In turn, the Security Committee serves as a permanent collaboration body that assists the government and ministries in coordinating comprehensive security. It thus serves as a vital link bringing together ministries, security agencies, business representatives and NGOs (Finnish Government 2025, p. 40).

Beyond these institutional arrangements, a primary pillar of Finland's approach is that of strengthening psychological resilience as one of seven vital functions. The strategy defines it as "the ability of individuals, communities and society to withstand the stress caused by crisis situations and to recover from their impacts" (Finnish Government 2025, p. 22). With the individual being at the centre of this vital function, Helsinki especially considers individual, societal and institutional trust as well as critical media literacy as cornerstones of societal resilience in this domain, and stresses that authorities maintain this trust through their actions and communication. Indeed, and while not entirely attributable to Russia's full-scale invasion of Ukraine, surveys point to a high level of societal resilience among Finns: In autumn 2025, 78 per cent of respondents agreed that Finns should take up arms if attacked, even if the outcome seemed uncertain, and 80 per cent said they would contribute to national defence according to their respective abilities. While confidence is somewhat lower at the individual level, numbers still point towards a strong level of preparedness with 79 per cent consider-

ing society well prepared for crises, whereas 67 per cent rated their own knowledge and skills as adequate (ABDI 2025, pp. 22, 24, 50–51).

Beyond these institutional mechanisms alone, it also treats the population's functional capacity to act and willingness to contribute as vital functions with their own tasks and regular monitoring, while joint courses for decision-makers from across sectors help build and maintain the personal networks on which this architecture has relied for well over six decades (Finnish Government 2025, p. 23; ABDI 2025, p. 8).

Admittedly, for Austria specifically, Finland's proximity to an adversarial Russia and its long-standing tradition of whole-of-society defense readiness limit direct comparisons. Nevertheless, the Finnish experience offers valuable lessons on how societal resilience can be organised, implemented, sustained and communicated. Importantly, the Finnish case highlights that mapping responsibilities, clarifying issue ownership and regular exercises constitute the cornerstones of resilience in practice. In this respect, Austria's Federal Crisis Security Act (Bundes-Krisensicherheitsgesetz) already obliges federal ministers to draw up crisis plans and test them in regular exercises (B-KSG 2023, § 12), but the Finnish model illustrates how such obligations can be further operationalised through measures such as a published map assigning tasks to lead ministries, agreements involving businesses, municipalities and civil society organisations, and an annual report to the state leadership that tracks implementation task by task and thus makes progress visible.

Lithuania – Flexibility under Pressure

Similarly to Finland's case, Lithuania's approach to hybrid threats is shaped by the country's historical experience of war and external coercion. This historical experience helps explain the country's emphasis on identifying and naming hybrid threats explicitly. Currently, present day pressure is understood as operating across several interconnected domains, including information warfare, cyber operations, energy and economic coercion, espionage and kinetic operations, with balloon and drone warfare increasingly emerging as an additional frontier. Lithuania's national intelligence services recently confirmed the breadth of this threat environment, ranging from drone incursions and information operations to cyberattacks and hostile intelligence activity, while assessing the conventional military threat as likely to remain low, at least in the near term (VSD and AOTD 2026, pp. 5–6).

Nevertheless, especially the aerial dimension has escalated rapidly. Lithuanian authorities detected three balloons from Belarus in 2023, 184 in 2024 and around 700 in 2025, together with some 200 drone intrusions in 2025 (European Parliament 2025, p. 1). By December 2025, these incursions had caused 19 airport closures (European Parliament 2025, p. 1). Previously, civilian radars of the air navigation service could not detect the balloons, so the military took over monitoring instead. According to officials, the balloons fly at altitudes of up to 11 kilometres, emit no heat signature and transmit only brief GPS signals (Deveikis 2025).

The drone incursions present a somewhat different challenge. Lithuanian intelligence assesses that the two Russian Gerbera drones that crashed in Lithuania on 10 and 28 July 2025 entered its airspace accidentally after being diverted from their routes towards Ukraine by technical malfunctions or electronic warfare. Regardless, the fact that one of the drones carried an explosive charge underscores the potential threat level emanating from such incursions (VSD and AOTD 2026, p. 29).

The aforementioned balloons, on the other hand, are seen as a deliberate instrument. The intelligence services assess that the Belarusian regime could prevent the smuggling but exploits it for political gain, much as it orchestrated the migration crisis of 2021 (VSD and AOTD 2026, pp. 39–40). This further supports the demand to treat Belarus as an active actor rather than a merely passive conduit for Russian pressure. Specifically, the Russian and Belarusian military-industrial complexes are deeply integrated (VSD and AOTD 2026, p. 24), and the European Parliament describes Belarus as a

platform for Russia's hybrid operations against Europe (European Parliament 2025, p. 1).

Importantly, the spillover risk is growing as Russian production capabilities continue to expand. By August 2026, Ukrainian military intelligence estimated that Russia was producing around 3,000 jet-powered Geran-4 and Geran-5 strike drones monthly. The scale of their operational use has also increased accordingly. Indeed, Russia launched more than 8,000 Shahed-type UAVs, including decoys, against Ukraine in May 2026 alone, while the growing shift towards faster jet-powered variants was reflected in the use of more than 2,800 such drones in August (VSD and AOTD 2026, p. 29; Anokhin 2026, pp. 6, 8, 15; Shymkiv et al. 2026). Yet, existing air defences were conventionally designed for helicopters and missiles. The commander of the Lithuanian Armed Forces, Raimundas Vaikšnoras, asked publicly whether the country should exhaust its arsenal on balloons and leave its air defence exposed (Deveikis 2025). The Ukrainian experience meanwhile underscores the need for cheaper and more adaptable means of countering large numbers of low-cost aerial threats. Meanwhile, in September 2025, Lithuanian parliament passed a law that allows the armed forces to shoot down any drone violating Lithuanian airspace which took effect in October 2025 (Sytas 2025). Shortly after, in December 2025, Vilnius declared a nationwide emergency situation over the balloons and authorised the shooting down of unmanned flying objects (European Parliament 2025, p. 1; Deveikis 2025). With the legal basis in place, Vilnius turned to detection and interception, fast-tracking the purchase of interceptor drones and radars and testing several systems in parallel, since drone technology changes within weeks (AdriaDefense 2026). On 15 September 2026, NATO air policing jets shot down a drone carrying explosives over central Lithuania, the first such interception over Lithuanian territory (Jakučionis 2026), although scrambling fighter jets against a single drone yet again underlined the cost problem. The updated National Security Strategy, built on total defence and with societal resilience as one of its three pillars, remains under parliamentary consideration after its first reading in March 2026 (Seimas 2026).

For Austria, Lithuania demonstrates above all how quickly legal and operational frameworks must adapt to an evolving aerial threat. Vienna's own Risk Monitor cites the drone-related shutdown of Munich Airport in October 2025 as evidence that the hybrid conflict has reached Europe itself (Tanner 2026, p. 10). Vienna has already begun expanding its detection and counter-drone capabilities and is developing a more comprehensive national framework. The practical lesson for Vienna, however, concerns the order of steps to be taken. Vilnius clarified the legal authority to shoot down drones during an airspace incursion before procuring interceptor systems. Only then did Lithuania test several such systems in parallel instead of committing to one solution only.

Poland – Resilience through Participation

Like Lithuania, Poland is exposed to hybrid pressure across several domains at once, with cyber, subversive and informational activities reinforcing one another. In 2025, Poland's government CSIRT GOV registered more than 23,000 reports and confirmed some 5,000 incidents in public administration, 26 per cent more than in the previous year (Ministry of Digital Affairs Poland 2026, pp. 10–11).

Beyond cyberspace, the Internal Security Agency (ABW) reports that Russian services recruit individuals motivated by financial gain through messaging apps such as Telegram, pay them in cryptocurrencies and increasingly work through organised criminal networks (ABW 2026, p. 13). In addition, the ABW documents the online radicalisation of minors and young adults, catalysed by such messaging apps as well as gaming forums (ABW 2026, p. 22). Moreover, satellite navigation in the Tricity area around Gdańsk has faced serious disruptions. In May and June 2026, multi-hour interference across all GNSS bands occurred on 70 per cent of days, which the National Institute of Telecommunications attributes to electronic warfare in the Baltic Sea region (IŁ-PIB 2026). At the regional level, Baltic undersea infrastructure remains exposed as well, even though Lithuanian intelligence has not linked recent

damage to undersea infrastructure to deliberate action by ships travelling from or to Russian ports (VSD and AOTD 2026, pp. 30–31).

The informational dimension further adds pressure. Specifically, the ABW lists undermining public trust in the state, polarising and intimidating society and fueling anti-European and anti-NATO sentiment among the priorities of Russian services in Poland (ABW 2026, p. 12), and it warns that platform recommendation algorithms entrench extreme views (ABW 2026, p. 21).

Warsaw's response, just like in Helsinki, is built on close cooperation between the state and civil society. The Advisory Council for Resilience to International Disinformation, established by ministerial order in September 2024, held its first meeting in April 2025. Its 22 experts were recommended by NGOs and universities, and it connects the administration with academia, local governments, civil society and business (MFA Poland 2025). In practice, the council submitted 13 recommendations in December 2025, ranging from the adoption of a national strategy against international disinformation to media literacy in school curricula, and noted that most disinformation content remains legal under Polish law (Advisory Council for Resilience 2025).

These initiatives are embedded in a civil protection framework with a firm legal and financial basis. The Civil Protection and Civil Defence Act, in force since 1 January 2025, designates at least 0.3 per cent of GDP annually for civil protection (Civil Protection Act 2024, Art. 155) and names civil society actors such as the Polish Red Cross, volunteer fire brigades and scouting organisations as civil protection entities (Civil Protection Act 2024, Art. 17). Accordingly, the government adopted a first civil protection programme in May 2025 with a budget of ca. EUR 3.9 billion for 2025 and EUR 3.9 billion for 2026 (Council of Ministers 2025a, p. 49; 2025b).

> Youth participation becomes a counter-hybrid measure in itself.

One innovative element in Poland's resilience building is the Youth Resilience Council, which brings young people directly into Poland's resilience work. The Foreign Ministry presents the initiative as a model for cooperation with the younger generation in responding to emerging information and digital threats, including those associated with social media and artificial intelligence (MFA Poland 2026b). The need is well documented: 44 per cent of Polish teenagers report difficulties in distinguishing true from false information online, and many of the 33 foreign disinformation operations uncovered in 2024 targeted young voters specifically (Litwiński et al. 2026, pp. 1–2).

Warsaw also invests in counter-narratives abroad. Poland's Russian-language news service (Vot Tak) team of public broadcaster TVP recorded more than 818 million views in 2025 and launched a Romanian-language channel for Moldova in February 2026 (MFA Poland 2026a).

For Austria, the Polish case shows that restrictions imposed from the top without the participation of young people are likely to be circumvented. Research on young people finds that a sense of agency and real influence on public decisions is one of the key protective factors against information manipulation (Litwiński et al. 2026, p. 15). In that sense, youth participation becomes a counter-hybrid measure in itself by ensuring ownership of the rules and debates young people are affected by. Austria could combine a standing youth resilience format with a civil society council on disinformation and give both the kind of legal and budgetary basis that Poland has created for civil protection.

Austria – Building on Solid Foundations

Naturally, Austria finds itself in highly different geographic and historical circumstances from the countries assessed thus far. And while, as stated previously, its neutrality does not offer any protection against hybrid pressure, threats are often perceived as distant and intangible among the population. Yet the drone-related closures of Munich Airport

in October 2025 and, more recently, Leipzig Airport show that these threats already manifest in Austria's wider to immediate neighbourhood. (Tanner 2026, p10.; Bewarder et al. 2026). At the same time, Austria has built a solid framework in recent years. The annual Risk Monitor of the Ministry of Defence maps the threat environment, the Austrian Security Strategy 2024 sets the strategic direction and is currently being revised with input from a citizens' dialogue forum, and the Federal Crisis Security Act (B-KSG) has created a whole-of-state coordination structure for the first time. Furthermore, the Critical Entities Resilience Act (RKEG), that came into force in January 2026, extends binding resilience obligations to operators of critical infrastructure. Nevertheless, the state and its emergency services appear better prepared than large parts of civil society, where much hybrid activity ultimately takes effect. The survey data in the section on Finland point to a similar gap between collective and individual preparedness, so the dynamic in Austria is not per se unusual. But, and especially given Austria's federal structure, narrowing this very gap will require coordination across all levels of government and civil society. Building on this framework, Austria could consider several further steps.

Map and Exercise Responsibilities

The B-KSG already obliges federal ministers to draw up crisis plans and test them in regular exercises (B-KSG 2023, § 12), and it provides for regular situation reports as well as an annual report to the federal government. In this regard, Austria is on the right path, and Finland offers an appropriate model for its further development. Specifically, the Finnish practice of assigning every strategic task to a lead ministry suggests that a consolidated and publicly accessible overview of responsibilities may add further value. Such an overview could also reflect the roles of the Länder, municipalities, operators of critical infrastructure and civil society organisations. The ongoing revision of the Security Strategy may offer a suitable opportunity for this. Joint exercises with partner countries would complement these efforts, since they reveal practical shortcomings at an early stage. Vienna may also further draw from the Finnish approach of joint courses for decision-makers from different relevant sectors, which not only transfer practical knowledge, but also establish helpful personal contacts before a crisis actually occurs.

Keep Pace with the Aerial Threat

Austria has already taken important steps in this field. The armed forces are building up counter-drone capabilities, an interministerial working group has been developing a whole-of-state counter-drone strategy since early 2026, and Vienna has announced legal amendments that would allow operators of critical infrastructure to act against drones. The Lithuanian experience largely confirms this course. Vilnius fast-tracked the procurement of interceptor drones and radars once the legal basis was established, which suggests that the announced legal amendments deserve priority. Yet, given how quickly drone technology evolves, Austria would be advised to consider procurement procedures that allow several systems to be tested in parallel, and adapted at short intervals. In addition, the interministerial exercise planned for this year could develop into a regular format, helping to ensure smooth cooperation between police, military and private operators. Planned investments could also be reviewed regularly, not least with a view to the cost of a single interception.

Embed Youth Participation in Resilience Policy

With the planned minimum age of 14 for social media platforms and a planned compulsory subject on media and democracy in secondary schools, Austria is addressing young people's digital vulnerabilities. An age limit alone does not reach all relevant channels, however, as the Polish ABW has documented the online radicalisation of minors via messaging apps and gaming forums (ABW 2026, p. 22). Nevertheless, the Polish case suggests that such measures may prove more durable when young people are involved in their design and implementation. Austria already has well-established participation structures, including the Austrian National Youth Council (Bundesjugendvertretung) and the Austrian Youth Strategy. Building on these, a dedicated

youth format on resilience and digital threats would help identify emerging risks at an early stage, while giving young people a sense of agency (cf. Litwiński et al. 2026, p. 15). Such a format could accompany the implementation of the social media age limit and feed its findings into the revised Security Strategy.

Further Institutionalise Dialogue on Disinformation

Austria's Security Strategy recognises foreign information manipulation as a threat, and the current government programme foresees further measures against disinformation. To this end, Austria could consider a standing advisory format modelled on Poland's Advisory Council for Resilience to International Disinformation, bringing together public authorities, academia, media, local governments and civil society organisations. Such a body could pool existing expertise, formulate recommendations and, in turn, strengthen trust between the state and civil society. Stable and independent funding for the participating organisations would be an important prerequisite for its credibility.

In sum, Austria already possesses the strategic, legal and institutional foundations for strengthening its resilience against hybrid threats. Still, it remains imperative to anchor these foundations more firmly in society and to keep them adaptable to a rapidly changing threat environment. The three case studies offer different lessons in this respect. Finland demonstrates the value of clearly assigned responsibilities and regular exercises, Vilnius the need to adapt legal and operational frameworks quickly, whereas the Polish case highlights the contribution of young people and civil society. Independent research institutions, academia and civil society organisations can help contribute to this process by bringing international experience into the national debate and fostering exchange between policymakers and the public. While Vienna has built solid foundations, the task at present is to develop them into durable structures that give civil society a more systematic role in national resilience.

About the Author

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. In this context, his work increasingly addresses hybrid threats.

© Austria Institut für Europa und Sicherheitspolitik, 2026

All rights reserved. Reprinting or similar or comparable use of publications of the Austrian 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

Bibliography

1 ABDI (Advisory Board for Defence Information) (2025): Finns' Opinions on Foreign and Security Policy, National Defence and Security. Bulletins and Reports 2025:3, Ministry of Defence, Helsinki, https://julkaisut.valtioneuvosto.fi/server/api/core/bitstreams/5a00c8c9-209c-4f07-a9b8-7178aea7f6ee/content

2 ABW (Internal Security Agency) (2026): Polish Internal Security Agency (ABW) 2024–2025. Selected Activities. Warsaw, https://www.abw.gov.pl/download/25/4876/ABWreport20242025.pdf

3 AdriaDefense (2026): Lithuania Fast-Tracks Drone Interceptors and New Radars. AdriaDefense Desk, 2 September 2026, https://www.adriadefense.com/lithuania-fast-tracks-drone-interceptors-and-new-radars/

4 Advisory Council for Resilience to International Disinformation (2025): Recommendations of the Advisory Council for Resilience to International Disinformation to the Minister of Foreign Affairs on countering disinformation in the information environment. Ministry of Foreign Affairs of Poland, 31 December 2025, https://www.gov.pl/web/diplomacy/recommendations-of-the-advisory-council-for-resilience-to-international-disinformation-to-the-minister-of-foreign-affairs-on-countering-disinformation-in-the-information-environment

5 Anokhin, I. (2026): August 2026 Updated Analysis of Russian Shahed-type UAV Deployment Against Ukraine. Institute for Science and International Security, Washington, DC, 8 September 2026, https://isis-online.org/uploads/isis-reports/documents/August_2026-Updated-Analysis-of-Russian-Shahed-type-UAVs-Deployment-Against-Ukraine_Final.pdf

6 B-KSG (2023): Bundes-Krisensicherheitsgesetz [Federal Crisis Security Act], BGBl. I Nr. 89/2023 as amended by BGBl. I Nr. 50/2025, https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20012321

7 Bewarder, Manuel, Jörg Diehl, Florian Flade, and Roman Lehberger (2026): 'Versuchter Drohnenanschlag in Leipzig: Verdächtiger soll enge Verbindung zu GRU-Oberst gehabt haben'. tagesschau.de, September 15. https://www.tagesschau.de/investigativ/ndr-wdr/leipzig-drohne-saboteur-100.html.

8 Civil Protection Act (2024): Ustawa z dnia 5 grudnia 2024 r. o ochronie ludności i obronie cywilnej [Act of 5 December 2024 on Civil Protection and Civil Defence]. Dziennik Ustaw 2024, poz. 1907, https://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU20240001907/T/D20241907L.pdf

9a Council of Ministers of the Republic of Poland (2025a): Uchwała nr 72 Rady Ministrów z dnia 27 maja 2025 r. w sprawie zatwierdzenia Programu Ochrony Ludności i Obrony Cywilnej na lata 2025–2026 [Resolution No. 72 of 27 May 2025 approving the Civil Protection and Civil Defence Programme 2025–2026]. Monitor Polski 2025, poz. 541, https://eli.gov.pl/eli/MP/2025/541/ogl

9b Council of Ministers of the Republic of Poland (2025b): Uchwała nr 151 Rady Ministrów z dnia 4 listopada 2025 r. zmieniająca uchwałę w sprawie zatwierdzenia Programu Ochrony Ludności i Obrony Cywilnej na lata 2025–2026 [Resolution No. 151 of 4 November 2025 amending the resolution approving the Civil Protection and Civil Defence Programme 2025–2026]. Monitor Polski 2025, poz. 1143, https://isap.sejm.gov.pl/isap.nsf/download.xsp/WMP20250001143/O/M20251143.pdf

10 Deveikis, J. (2025): Chronology of contraband balloon 'hybrid attack' – here's what you should know. LRT English, 11 December 2025, https://www.lrt.lt/en/news-in-english/19/2771303/chronology-of-contraband-balloon-hybrid-attack-here-s-what-you-should-know

11 EEAS (European External Action Service) (2026): 4th EEAS Report on Foreign Information Manipulation and Interference Threats: Dismantling the FIMI House of Cards. Brussels, March 2026, https://euvsdisinfo.eu/eeas-4th-fimi-threat-report-march-2026/

12 European Parliament (2025): European Parliament resolution of 18 December 2025 on the continuous Belarusian hybrid attacks against Lithuania (2025/3025(RSP)), P10_TA(2025)0345. Official Journal of the European Union, C/2026/2161, 6 May 2026, http://data.europa.eu/eli/C/2026/2161/oj

13 Finnish Government (2025): Security Strategy for Society. Government Resolution, 16 January 2025. Publications of the Finnish Government 2025:3, Security Committee, Helsinki, https://urn.fi/URN:ISBN:978-952-383-817-8

14 IŁ-PIB (Instytut Łączności – Państwowy Instytut Badawczy) (2026): Analiza zakłóceń systemów nawigacji satelitarnej (GNSS) w Trójmieście [Analysis of GNSS interference in the Tricity area]. 24 August 2026, https://www.gov.pl/web/instytut-lacznosci/analiza-zaklocen-systemow-nawigacji-satelitarnej-gnss-w-trojmiescie

15 Jakučionis, S. (2026): NATO jets shoot down drone that entered Lithuanian airspace. LRT English/BNS, 15 September 2026, https://www.lrt.lt/en/news-in-english/19/3053032/nato-jets-shoot-down-drone-that-entered-lithuanian-airspace

16 Litwiński, P., Dachowski, M., Miśniakiewicz, H. & Oleszyńska, J. (2026): Młode pokolenie w państwie przyfrontowym. Rekomendacje dotyczące wdrożenia agendy „Młodzież, Pokój i Bezpieczeństwo" w Polsce [The Young Generation in a Frontline State: Recommendations for Implementing the Youth, Peace and Security Agenda in Poland]. Policy Brief,

Casimir Pulaski Foundation, Warsaw, 21 April 2026, https://pulaski.pl/wp-content/uploads/2026/04/YPS-Policy-Brief_PL_MD_HM_JO.docx.pdf

17 MFA Poland (Ministry of Foreign Affairs of the Republic of Poland) (2025): Council for Resilience, joint initiative by MFA and civil society organisations against international disinformation, begins operation. 3 April 2025, https://www.gov.pl/web/diplomacy/council-for-resilience-joint-initiative-by-mfa-and-civil-society-organisations-against-international-disinformation-begins-operation

18 MFA Poland (Ministry of Foreign Affairs of the Republic of Poland) (2026a): Telewizja Polska launches Romanian-language version of "Vot Tak. Moldova". 4 February 2026, https://www.gov.pl/web/diplomacy/telewizja-polska-launches-romanian-language-version-of-vot-tak-moldova

19 MFA Poland (Ministry of Foreign Affairs of the Republic of Poland) (2026b): Deputy Prime Minister Radosław Sikorski at "The War for Minds. Fear, Subversion, Disinformation" conference in Sejm. 8 June 2026, https://www.gov.pl/web/diplomacy/deputy-prime-minister-radoslaw-sikorski-at-the-war-for-minds-fear-subversion-disinformation-conference-in-sejm

20 Ministry of Digital Affairs Poland (2026): Sprawozdanie Pełnomocnika Rządu do Spraw Cyberbezpieczeństwa za 2025 rok. Tom I – Podsumowanie zarządcze [Report of the Government Plenipotentiary for Cybersecurity for 2025, Vol. I – Executive Summary]. Warsaw, https://www.gov.pl/attachment/73507c5b-eab8-432d-ac3a-890061346e31

21 Ministry of the Interior of Finland (2023): National Risk Assessment 2023. Publications of the Ministry of the Interior 2023:6, Helsinki, https://urn.fi/URN:ISBN:978-952-324-610-2

22 Ministry of the Interior of Finland (2026), "National Risk Assessment", Sisäministeriö, https://intermin.fi/en/rescue-services/preparedness/national-risk-assessment.

23 Seimas of the Republic of Lithuania (2026): Seimas spręs dėl Nacionalinio saugumo strategijos atnaujinimo [The Seimas will decide on updating the National Security Strategy]. Press release, 17 March 2026, https://www.lrs.lt/sip/portal.show?p_r=35435&p_k=1&p_t=294249

24 Shymkiv, K., Harward, C., Mappes, G., Sher, A. & Hird, K. (2026): Russian Offensive Campaign Assessment, August 12, 2026. Institute for the Study of War & AEI's Critical Threats Project, 13 August 2026, https://www.criticalthreats.org/analysis/russian-offensive-campaign-assessment-august-12-2026

25 Sytas, A. (2025): Lithuania authorises army to shoot down drones violating its airspace. Reuters, 23 September 2025, https://www.reuters.com/business/aerospace-defense/lithuania-authorises-army-shoot-down-drones-violating-its-airspace-2025-09-23/

26 Tanner, K. (2026): Foreword. In: Federal Ministry of Defence (BMLV): Risk Monitor 2026. The End of Order? Vienna, https://verteidigungspolitik.at/documents/475963/0/Risk+Monitor+2026+Digital.pdf/2f87cebd-1422-5b98-d65c-eda7f066986e

27 VSD (State Security Department of the Republic of Lithuania) & AOTD (Defence Intelligence and Security Service under the Ministry of National Defence) (2026): National Threat Assessment 2026. Vilnius, https://www.vsd.lt/wp-content/uploads/2026/03/2026-GR-ENG-El.pdf