ISBN 978-9934-619-73-1

Countering Information Influence Operations in the Nordic-Baltic Region

PREPARED AND PUBLISHED BY THE

NATO STRATEGIC COMMUNICATIONS CENTRE OF EXCELLENCE

ISBN: 978-9934-619-73-1

Authors: Johannes Lindgren, James Pamment, Angela Palmer, Sanda Svetoka, Elīna Lange-Ionatamišvili
Contributors: Sandra Hiller, Päivi Tampere
Project Manager: Johannes Lindgren
Content Editor: Merle Anne Read
Design: Inga Ropša

Riga, January 2026

NATO STRATCOM COE
11b Kalnciema iela,
Riga, LV1048, Latvia
stratcomcoe.org
@stratcomcoe

Countering Information Influence Operations in the Nordic-Baltic Region

Contents

Foreword 5

Executive Summary 6

Introduction 7

- Outline 8

Methodology 9

- Selection 10
- Limitations 10

Regional Profile 11

- Framework, policy, and coordination 12
- Situational awareness 13
- Resilience building 14
- Communicative response 15
- Disruptive response 16
- International cooperation and joint countering 16

Country Profiles 18

- Denmark 18
- Estonia 20
- Finland 24
- Iceland 28
- Latvia 32
- Lithuania 36
- Norway 39
- Sweden 43

Discussion 48

Conclusion 50

Bibliography 51

- Main report 51
- Country profiles 51

Foreword

This research forms part of the NATO Strategic Communications Centre of Excellence´s ongoing effort, begun in 2016, to understand malign foreign influence in the Nordic-Baltic region (Denmark, Estonia, Finland, Iceland, Latvia, Lithuania, Norway, and Sweden – the NB8). Its core objective has been to map the capabilities of the Nordic-Baltic countries and to compare their approaches to countering information influence.

The Nordic-Baltic region shares centuries of historic trade and socio-cultural ties. Following the fall of the Soviet Union, Nordic-Baltic cooperation was renewed; initially as '5 + 3' but later as '8', reflecting a group of nations united not only by geography but by liberal democratic values and similar aspirations and challenges.

Fifteen years ago, the need for such research might have seemed less pressing or even unreasonable. The world and the region were very different back then. There was less consensus on what to expect from the threat actors, and less awareness of hybrid methods of 'below the threshold' influence and how open societies could be manipulated by those seeking to undermine them. But now, as this document demonstrates, there is a great degree of similarity in how Nordic-Baltic societies and governments perceive these threats and their role in safeguarding national and regional security. The countries share common values, governance principles, and threat assessments. Their collective ability to act and share information has been furthered by Finland's and Sweden's decision to join NATO.

As we look ahead, challenges to our information environments will most likely intensify amid ongoing geopolitical turbulence. Manipulation will become more sophisticated through emerging technologies. And we already see that information influence is often paired with other hostile actions such as cyberattacks, physical sabotage, and disruption of critical infrastructure. Our agility, flexibility, and commitment to cooperate will remain vital.

We trust that this report will reinforce confidence in the resilience of the NB8 while identifying practical areas for further growth and improvement, particularly through joint training and regional experience sharing.

Executive Summary

The Nordic-Baltic (NB8) countries have implemented various frameworks, policies, and coordination mechanisms to address the issue of information influence operations (IIOs).[1] Most countries have national security strategies coupled with specific strategies or concepts to tackle IIOs, with resilience being a central theme in these frameworks.

Resilience can refer to both public awareness and critical thinking, as well as the ability of state institutions to manage incidents effectively. Resilience building involves educating the public, particularly focusing on media literacy and critical thinking. Non-state actors, such as NGOs and civil society, play a crucial role in enhancing societal resilience through various initiatives, often with government support. Media sector cooperation is also significant, with states engaging in information exchange and assistance.

All the NB8 countries engage in monitoring and situational analysis, primarily by defence and intelligence bodies. Situational awareness products are shared domestically and internationally on an ad hoc or regular basis. However, resources for continuous monitoring are lacking in some cases. Legislative measures for addressing IIOs are limited. EU laws and national media regulations often form the basis for limiting foreign state media influence. Public coordination structures vary across the region, ranging from formal to informal, with the involvement of various ministries and agencies.

Strategic communications is another key concept in several countries. Communication responses are mostly case by case, with affected agencies often responsible for managing responses to IIO incidents. Civil society organisations often lead fact-checking and debunking efforts. Attribution of IIOs can be direct or indirect, depending on the severity of the situation. Disruptive measures include sanctions against media outlets, amendments to criminal codes and national security acts, and regulation of language and the media. There is a transition towards more direct legal action against IIO activities.

International cooperation takes place through multilateral forums, for example in the EU and NATO, as well as bilateral cooperation among regional allies. Challenges include resource strain from multiple parallel forums, duplication of efforts, and balancing national interests with joint responses.

Key takeaways for other countries seeking to learn from the NB8 region include adopting a whole-of-society approach, involving civil society and the media, fostering close public coordination, and enhancing citizen resilience through communication and education initiatives. Challenges involve balancing freedom of speech with disruptive measures, assisting the media without being overly directive, managing civil society involvement, deciding when to respond, and how to prioritise international cooperation.

The NB8 region has potential for deeper cooperation in countering IIOs, which could include establishing shared capability development frameworks, capability leadership among member countries, conducting joint exercises, and developing coordinated response projects. This would complement existing international efforts and enhance the regional capacity to address these threats effectively. In conclusion, the NB8 countries demonstrate a strong approach to combating IIOs, with a focus on resilience building and effective coordination. Future research and collaboration can further strengthen capabilities and share best practices in this area.

1 Information influence operations (IIOs) are understood in this report as deliberate efforts to manipulate public opinion, undermine trust, and exploit social vulnerabilities, often to the benefit of a hostile state actor. They involve coordinated, illegitimate behaviours which exploit the openness of democratic societies.

Introduction

The Nordic-Baltic region comprises eight Northern European countries with a shared history, culture, and geography. The five Nordic states (Denmark, Finland, Iceland, Norway and Sweden) are known for their 'Nordic model', a form of governance associated with freedom of speech and secularism, strong social welfare, high levels of democratic transparency, and strong societal trust. The three Baltic States (Estonia, Latvia, Lithuania) share a common past of Soviet occupation, and since restoration of their independence have been close partners in foreign and security policy, as well as economic development and infrastructure.

As small European countries, the Nordic-Baltics share a strong commitment to multilateralism and integration, and are highly educated and technologically advanced, have low levels of corruption, and are generally open societies. As of 2024, all Nordic-Baltic countries are NATO allies, and all are either members of the European Union or the European Economic Area (EEA; Iceland, Norway). To maximise their opportunities for influence in the region, Nordic-Baltic Eight cooperation has existed since the 1990s as a platform for political coordination. The NB8 consists of a multilayered format that enables many levels of government, from heads of state to authorities, to convene around strategically relevant topics.

During the Cold War, Soviet propaganda in the region framed NATO as an aggressor, sought to undermine the neutrality of Nordic countries, and delegitimised independence movements. Post-Cold War, the rights of ethnic Russians and Russian speakers based in the Baltic States have been a continual vector for the Russian Federation to conduct IIOs. The Soviet Union's shared history with the Baltic countries has been a particular sore point: for example, in 2007 when Estonia relocated the Soviet-era Bronze Soldier memorial, Russia responded with crippling cyberattacks and disinformation accusing the country of Nazism. Migration and integration policies have dominated Russian disinformation strategies, as well as falsehoods about NATO's military presence in the region, and claims of Russophobia, fascism, and censorship.

Building in particular upon the Bronze Soldier experience, NB8 countries were early to build structured resilience to Russian IIOs, with the support of NATO. Estonia established the Cooperative Cyber Defence Centre of Excellence in 2008; Lithuania, the NATO Energy Security Centre of Excellence in 2012; Latvia, the Strategic Communications Centre of Excellence in 2014; and Finland, the European Centre of Excellence for Countering Hybrid Threats in 2017. Since Russia's annexation of Crimea in 2014, the Baltic countries have also hosted NATO's Enhanced Forward Presence, consisting of multinational battlegroups designed to project deterrence.

Today the region is strategically important for both European and transatlantic security. With five countries sharing borders with Russia, conventional military threats and hybrid interference have been major drivers of increased political and military integration. Espionage, cyberattacks, diplomatic and economic coercion, airspace violations and GPS jamming, and interference with critical infrastructure such as underwater cables, as well as IIOs, are common both in the Baltic Sea region and in the High North. Hostile Russian activities that test resolve, detection capabilities, and response thresholds continually hold the threat of escalation over the region's countries. Since the full-scale invasion of Ukraine in 2022, and Finland's and Sweden's subsequent entry into NATO, tensions have heightened, with the region considered a probable target should Russia's war of aggression spread further into Europe.

In respect of Russian IIOs in particular, previous research noted a certain degree of similarity in regard to the Russian modus operandi used towards the countries in the

region.[2] This includes tactics such as the use of foreign media channels to spread disinformation in local languages, forged letters and false virtual meetings, and the portrayal of certain local alleged 'expertise' as the voice of reason in a certain country. Similarities can also be identified when it comes to narratives including the support of existing local anti-establishment rhetoric. NB8 countries are portrayed as 'colonised' and being 'controlled' by the United States, and narratives are directed against the West as a whole portraying NATO and its allies as being weak and incapable of resisting Russia.

China has also projected its own power in the region, albeit with the long-term objective of exerting influence through investment, technology exchange, and diplomatic pressure rather than direct military coercion. Sweden has long been aware of espionage targeting its tech sector, while Lithuania experienced strong diplomatic and economic retaliation following its 2021 decision to allow the opening of a Taiwanese representation office in the capital, Vilnius. Fears over intellectual property theft, spying, and dual use technologies have led to the exclusion of Chinese companies from some sensitive technology areas, such as 5G. Chinese investments in ports and other critical infrastructure demonstrate the challenge of balancing inward investment with strategic security risks. China has also targeted NB8 countries through IIOs, for instance in relation to local politics in Sweden and towards Lithuania in the context of the opening of the Taiwanese Representative Office.

Given that hostile actors target the whole region with IIOs, it is important to understand how the threat is countered across the Nordic-Baltic region. Thus, in this report we **seek to shed light on the strategic approach as well as the pre-emptive and reactive measures being taken by the countries in the region.** The **purpose** of the report is, through examining the approaches of NB8 countries dealing with IIOs, to provide NB8 countries and others with best practices, indicate possible areas for improvement, and investigate opportunities for deepened regional cooperation. To support this aim, the following research questions were formulated:

1. What type of strategic approach is guiding the NB8 countries in their efforts to counter information influence operations (IIOs)?
2. What form of pre-emptive and reactive measures are being taken by the NB8 countries to counter IIOs?
3. What are the key lessons learned for other countries?
4. What should the NB8 countries do to improve their capabilities in countering IIOs?

Outline

This report consists of **two main sections**. The first summarises the collective results and assesses the measures from a regional point of view. The second provides insights into how each country in the NB8 is countering IIOs through short, detailed case studies. Following the main sections is a discussion that summarises the findings and outlines challenges and possible areas of improvement.

2 H. Mölder and V. Sazonov, 'Estonia.' In A. Ahonen, A. Bilal, Gjørv Hoogensen, J. Jurāns, M. Kragh, K.K. Krūmiņš, E. Lange-Ionatamishvili, B. Liubinavičius, K. Mikulski, H. Mölder, J.G. Ólafsson, S.B. Ómarsdóttir, V. Sazonov, and J. Serritzlev, *Russia's Information Influence Operations in the Nordic-Baltic Region*. NATO Strategic Communications Centre of Excellence, November 2024. *https://stratcomcoe.org/pdfjs/?file=/publications/download/RUS-Info-Influence-Operations-in-Nordic-Baltic-DIGITAL-V2.pdf*.

Methodology

There is no single 'best' model for countering IIOs. Instead, this analysis focuses on understanding how organisations and systems are designed to address threats according to their specific mandates, priorities, and available resources. In this report we outline capabilities, approaches, and countermeasures, both at national level and across the region. **We avoid comparing individual countries with each other**, given that local contexts and guiding logics are slightly different even within a like-minded region such as the NB8. **However, we do outline similarities and differences on a regional level** to provide knowledge on best practices for other countries.

The main methodology guiding the work is qualitative, involving semi-structured interviews with key actors, supported by open source research. Analysis of the collected data is based on an **abductive approach** including both the identification and clustering of themes originating from the collected data and predetermined analytical categories based on a previous NATO StratCom COE publication, *A Capability Definition and Assessment Framework for Countering Disinformation, Information Influence, and Foreign Interference*, which outlined over 90 capabilities used to counter IIOs. The following analytical categories were constructed based on the framework and the collected data:

- **Framework, policy and coordination:** This includes the frameworks that NB8 countries apply to the issue of IIOs. It also outlines the type of public coordination which guides the work.

- **Situational awareness:** This includes the monitoring and situational analysis conducted by the countries in the region. It focuses on whether it is being done ad hoc or more systematically as part of a structure, as well as on the distribution of the analysis, both domestically and internationally.

- **Resilience building:** This includes measures taken to enhance the resilience of institutions and organisations as well as the general public towards IIOs. Also, it highlights to what extent cooperation with non-state actors such as the media and civil society is being conducted.

- **Communicative response:** This includes to what extent nations are engaging in strategic communication (debunking, fact checking, counter-narratives, etc.) as a response to an identified incident in the information environment. It also sheds light on the issue of attribution, as well as on which actor is doing the communication.

- **Disruptive response:** This includes to what extent countries in the region enforce legislative measures to disrupt IIOs. It includes sanctions, legislation targeting individuals, and legislation on language and media regulation.

- **International cooperation and joint countering:** This includes the international engagement of the NB8 countries, as well as the potential for future improvements in international cooperation.

These categories have been applied to the analysis of each country and to that of the region as a whole.

Selection

For this report we made several selections affecting the end result. This includes:

- **Selection of actors to interview:** For the purpose of getting a broad overview of each country's approach, we conducted interviews with civil and military actors both at agency and ministry level. However, given that the structures vary in each of the countries, the actors we met also differed to some extent. For most countries we met with (1) the Ministry of Defence; (2) the Ministry of Foreign Affairs; (3) the Prime Minister's Office or similar; (4) the defence forces. In some countries we also met with intelligence agencies, ministries of culture, media commissions, and country-specific agencies, depending on the relevance and availability of the actors. Furthermore, in rare cases researchers and experts were also interviewed to provide contextual information.
- **Focus on overall approach in peacetime:** The focus was not on war but rather peacetime. Thus, this affects the choice of constructed analytical categories, as well as the involvement of actors. For instance, there is a heavier focus on civil capabilities and approaches rather than those of the military.
- **Actor-agnostic approach:** In our analysis of the approaches of the countries, we do not specify whether strategies or measures are being set up towards a specific threat actor. Rather we lean on a general actor-agnostic approach to avoid complications in providing a general overview.
- **Updates made after July 2025 are not included in the report:** A lot of actions and measures are being initiated continuously in this space by the NB8 countries. Thus, this report only takes into account the work that has been done up until July 2025.

Limitations

We do not provide a fully comprehensive view of each country. This is due to the fact that (a) in some countries it was not possible to conduct interviews with some key stakeholders; (b) some information could not be shared by the countries due to sensitivities, and (c) our aim was not to provide a full list of everything each country is doing. Thus, this report **should not be considered as a fully comprehensive view of what each NB8 country, and the NB8 region as a whole, is doing to counter IIOs**. Rather it provides an overview of approaches based on selected categories.

Regional Profile

This section outlines how the Nordic-Baltic countries are countering IIOs in different analytical categories. The categories were based on gathered data and the capability definition and assessment framework mentioned above.

The section is divided into two parts. The first part includes a table visualising the main takeaways of each category. It uses colour coding to indicate how many countries (all, most, several, a few) are conducting a certain activity or have a certain capability (Table 1). The second part describes the activities of the countries in more detail.

Framework, policy, and coordination

Framework	Standalone legislation	Public coordination
Most states have a framework in place that either partially or fully addresses IIOs	A few states have a standalone legislation addressing IIOs	Most states have formal coordination structures convening on a regular basis

Situational awareness

Monitoring	Information sharing	Public release
All countries are engaged to varying degrees in some form of monitoring and situational analysis	Several countries provide reports and information frequently to their regional partners	In most countries, both the domestic and foreign intelligence services release declassified intel reports for the public to enhance societal awareness

Resilience building

Media literacy and critical thinking	Training	Financial support of NGOs
Most countries prioritise media literacy and critical thinking as part of their public resilience building	Several countries provide regular capability development training to strengthen the resilience of public institutions and other organisations	Several states provide **regular** grants aimed at strengthening NGOs and boosting civic resilience

Communicative response		
Response on case-by-case basis	**Actor responsible**	**Cooperation with the media**
Most countries base their communicative response on a case-by-case basis	In several states the agency which has been directly targeted has immediate responsibility for managing their response to any confirmed IIO	In a few states the government will advise, or provide contextual information, to the media sector in relation to an identified incident
Disruptive response		
Disruption	**Legal tools to limit IIOs**	**Media legislation**
All countries in the region have instituted disruptive measures in an effort to undermine the ability of external actors to infiltrate the domestic information environment	Several states have amended existing legislation, such as criminal codes and national security acts, to address activities which support external actors in their influence efforts	A few states have a legal mandate to intervene directly against service providers and block domains
International cooperation		
Regional coordination	**Joint countering**	**Information sharing**
Several states are in regular contact with their closest regional allies	A few states are in principle in favour of different forms of joint countering activities	All states point to the value of information sharing to build opportunities for further collaboration within the region

TABLE 1. Regional overview of counter-IIO activities based on analytical category.
Key: All states; most states; several states; a few states.

Framework, policy, and coordination

This section outlines the frameworks that NB8 countries apply to the issue of IIOs. It also outlines the type of public coordination which guides the work.

Most nations have a framework in place that addresses, either partially or in full, the issue of IIOs. These frameworks differ from each other: for a **few states** the national security strategy or similar is the only relevant guiding document for IIOs; **for most,** however, there is more than one framework or guiding strategic document. For these countries there is typically a national security strategy coupled with a more specific strategy or concept for addressing IIOs.

For most countries, resilience is a central approach to these frameworks. The meaning of resilience varies from state to state. In some cases the focus is on the resilience of the population, whereas in other instances its focus centres on the resilience of state institutions and organisations. In the context of domestic populations, this includes threat awareness, levels of source criticism, media literacy and critical thinking, trust in state institutions, and willingness to participate in a country's defence efforts. For state institutions or other organisations, it can refer to their ability to manage identified incidents and ensure that public services continue to function. **Strategic communications** is also a key guiding concept for **several states** – either as part of the overall framework or as a main strategy. It is frequently mentioned as a core capability for enhancing societal resilience.

Regarding the legislative aspects of the frameworks, **few states** currently have standalone legislation addressing IIOs per se. Instead, **several states** have separate legislative initiatives covering security threats, such as espionage, foreign propaganda, and subversion. In most cases a combination of EU laws and national media regulations have provisions to limit Russian state media in their respective media systems, though it should be noted that media policy across the region can be quite different.

All countries have some sort of public coordination structure in place. As with frameworks, the structure differs, both in terms of frequency and organisation of the coordination, as well as which actors are involved. **Most states** have formal structures in place that convene on a regular basis, **while a few** have more informal and ad hoc coordination processes. The involvement of actors also differs, where **several states** involve both relevant ministries and agencies in the same coordinating group, while a **few** have separate groups for agency-level and ministry-level coordination.

The purpose and nature of the coordination differs as well. **Most states** engage in operational coordination to be able to share information and take action in case of identified incidents. At the same time most states also convene to discuss more strategic perspectives related to IIOs, for example how to raise capabilities within a specific thematic area. The ministries, agencies, and other actors involved in the coordination bodies also differ; in several cases, the Prime Minister's Office is responsible, whereas in others a specific agency might be the lead for this particular area.

Situational awareness

This section outlines the monitoring and situational analysis conducted by the countries in the region. It focuses on whether it is being done ad hoc or more systematically as part of a structure, and on the distribution of the analysis, both domestically and internationally.

All countries within the Nordic-Baltic region are engaged to varying degrees in some form of monitoring and situational analysis. **Several states** have instituted distinct frameworks for observing activities within or targeting their respective information environments. At present most monitoring and situational analysis is undertaken by actors such as ministries of defence, the armed forces, and domestic and foreign intelligence bodies. **In a few states,** the highest government office, such as the Office of the Prime Minister, has oversight of monitoring activities and coordinates them. In many instances these activities are managed by dedicated units, committees,

or taskforce-based entities which, in addition to engaging in monitoring and situational analysis, also function as inter-agency bodies to coordinate activities with other relevant state actors.

In regard to the distribution of situational awareness products, it varies to a large extent within the region how frequently the information is shared domestically. Situational awareness reports are shared with regional partners on an ad hoc basis in response to discernible threats or to raise awareness of issues relevant to neighbouring countries. **Several countries** provide reports and information frequently to their regional partners, so as to ensure the timely exchange of information.

While situational analysis is given a high degree of priority within the region, **several countries** indicate that those units responsible for this activity currently lack the necessary resources to ensure robust and effective monitoring on an ongoing basis, including the need for financial resources and developing expert personnel to undertake these activities. **In most countries** both the domestic and foreign intelligence services release reports that are publicly available, to ensure there is broader societal awareness of any identifiable actors or threats to state interests.

A number of agencies have disclosed the presence of targeted Russian and Chinese IIOs within their respective countries. In this context situational analysis has acquired a degree of public transparency it might not otherwise have, as **most countries** in the region have come to prioritise threat awareness among their citizens in order to enhance public preparedness and responsiveness to IIOs.

Resilience building

This section outlines the work that the NB8 countries conduct to enhance the resilience of institutions and organisations as well as the general public towards IIOs. It includes to what extent cooperation with non-state actors such as media and civil society is being conducted.

Resilience building is considered to be a key priority for **all NB8 countries** in countering IIOs. One important part of this approach is the education of the public. In this space, **all NB8 countries** work in different ways to enhance the resilience of the population. Here **media literacy and critical thinking** are given a high priority among **most countries** through, for example, education in schools, conferences, and public communication campaigns**.**

In strengthening the resilience of public institutions or other organisations, **several NB8 countries** provide regular capability development training. These are coordinated mainly by the Prime Minister's Office or an equivalent, including in some cases the involvement of non-state actors such as NGOs or private companies. The training modules include elements on how to respond to IIOs, situational awareness training, and communications training.

One important part of enhancing the overall resilience of the country against IIOs is the **involvement of non-state actors**. This is a key aspect of the strategies developed in Nordic-Baltic countries. Civil society organisations are ideally positioned to enhance societal resilience in various ways, while the state assumes a supporting role via targeted funding, offering training and educational resources, and engaging with NGOs through meetings, workshops, and conferences. In this context, building stronger relationships with civil society organisations and the media sector have been given priority.

In this space **most states** collaborate with NGOs as part of their strategic communications and resilience activities, ranging from provision of advice on an ad hoc basis to

direct involvement in responses towards IIOs. Civil society involvement in resilience building is largely self-directed, as this enables NGOs to develop significant convening power by establishing peer networks and their ability to attract financial resources independently. These processes are often led by a central coordination hub within the government that oversees the whole policy area.

Several states provide regular grants aimed at strengthening NGOs and boosting civic resilience, in particular for those groups focusing on media literacy and education. While this speaks to the importance states place on NGO cooperation, the system creates an administrative burden for NGOs. Limited funding and awarding grants on a competitive basis means NGOs invest considerable time and effort sourcing funds for their activities.

The media sector in the region has a high level of professionalism and has a critical role in informing public agencies and countering IIOs. Within the Nordic-Baltic region, state engagement with the media sector is largely undertaken by individual ministries and agencies as part of their speciality areas. **Several states** will engage with media agencies as part of their efforts to address IIOs, exchanging information and guidance. While **most of these states** have informal connections with the media sector, a **few states** have established dedicated media reserves composed of local representatives to assist with their state resilience activities.

Communicative response

This section outlines to what extent nations are engaging in reactive communication (debunking, fact checking, counter-narratives, etc.) as a response to an identified incident in the information environment. It also sheds light on the issue of attribution and on which actor is doing the communication.

There is no explicit strategy for a direct communicative response for the vast majority of NB8 countries; instead states engage in communicative responses on a case-by-case basis, although the approach is generally of a careful nature. Often civil society and media actors are the ones engaging in communicative responses, for example by fact checking.

In **several states** the agency which has been directly targeted has immediate responsibility for managing their response to any confirmed IIO. Agencies will initiate some form of communication response to counter an incident if this is deemed appropriate. In those instances where an IIO constitutes a national security threat or national crisis, the relevant ministry or agency will typically escalate the issue to the lead coordinating body for the government, and it will assume responsibility for any communicative response as part of its response strategy. **A common approach** among states is to choose to avoid responding to IIOs with reactive communication where possible, as communicating about the incident has the potential to amplify the narratives being propagated by malicious actors. In both instances state agencies/ministries will usually decide the appropriate response on a case-by-case basis. Where possible, states will attribute specific IIOs to discernible actors. Sometimes the attribution is done directly by a government spokesperson, or in some cases by national intelligence agencies.

As previously mentioned, civil society organisations have an important function in responding to IIOs, largely due to their role in fact checking and debunking hostile narratives targeting the domestic information environment. The relationship between governments and the media is also an important factor enhancing official responses to IIO incidents. **In a few states** the government will advise, or provide contextual information, to the media sector in relation to an identified incident.

Disruptive response

This part focuses on to what extent countries in the region enforce legislative measures to disrupt IIOs. It includes sanctions, legislation targeting individuals, and legislation on language and media regulation.

All countries in the region have instituted disruptive measures in an effort to undermine the ability of external actors to infiltrate the domestic information environment. Among the most visible of these measures has been the imposition of sanctions against media outlets responsible for disseminating disinformation and propaganda. As most countries in the region are EU members, they have proactively enforced the EU media sanctions regime and suspended the broadcasting activities and licences of Kremlin-supported media outlets in Europe. EEA member states in the region have also chosen to align with the EU and enforce sanctions as part of their internal response to addressing malicious IIOs following the 2022 Russian invasion of Ukraine.

Within the region there has been a recent transition in the approach to taking legal action against IIOs. At a domestic level, **several states** have amended existing legislation, such as criminal codes and national security acts, to address activities which support external actors in their influence efforts. One example includes an amendment making it possible to take legal action against a domestic actor acting on behalf of or in collusion with a foreign intelligence service conducting information influence activities. Another example is the amendments to media and communication laws regulating public communications, specifically news publications, broadcasting, and online content. Here a **few states** have a legal mandate to intervene directly against service providers and block domains, for example on the grounds that the outlets could be linked to the Kremlin or constitute a threat to national security.

A more recent legislative measure which has been implemented by a **few states** relates to education and language. States have introduced legislative amendments to phase out Russian as a language of educational instruction within the domestic school system. The transition to the official state language has been introduced as a measure to prioritise that language as a resilience measure against malicious external influence.

In general there is variation in approaches to disrupting IIOs. The determining factors informing many of these measures are the state's experience of and exposure to IIOs, as well as domestic views on freedom of speech and expression.

International cooperation and joint countering

This section outlines the international engagement of the NB8 countries. This includes multilateral and bilateral cooperation, as well as the potential for future improvements in international cooperation.

Two of the most prominent forums where **several states** actively engage are the EU Rapid Alert System (EU RAS) and the newly formed NATO Rapid Response Group (NATO RRG). The EU RAS provides an organisational framework to facilitate information sharing between member states and EU institutions and, where appropriate, coordinates pan-European responses to incidents. The NATO RRG has a similar function, specifically as a collective response mechanism which includes NATO and Allied experts who detect, identify,

and coordinate responses to any information threats.

While acknowledging the importance of participating in multilateral frameworks, **most states** indicate that their involvement across multiple formats places considerable strain on government resources. A related issue is the duplication of state efforts, as unclear coordination mechanisms and state participation in too many parallel international forums were considered to be an ineffective strategy.

Bilateral cooperation among states in the region is active. **Several states** indicate they are in regular contact with their closest regional allies, with a **few states** communicating with regional partners on a daily basis. While the Nordic-Baltic states have reaffirmed their respective commitments to the EU and NATO formats, a **few states** indicate that the smaller, more informal engagement strategies they have established are often more effective in supporting some joint countering activities.

In regard to harnessing international networks for different kinds of cooperation, **all states** point to the value of information sharing to build opportunities for further collaboration within the region, as the effects of an IIO in one state may have ramifications across the NB8. **A few states** have expressed support in principle for engaging in joint activities countering IIOs, as there is a degree of consensus on the importance of cooperation in responding to IIOs in the region. However, states acknowledge this may not always be feasible, as each has its own distinct information environments, language, and communication culture. Instead, **all states** agree there is significant value in creating frameworks to facilitate information sharing and pooling expertise, as this will both enhance situational awareness within the region and enable states to build the necessary knowledge and skills to effectively counter IIOs.

In respect of capability development, bilateral exercises between regional partners have facilitated cooperation in building countering capabilities and enhancing the overall strategic position of Nordic-Baltic states against hostile actors. In this context, information sharing has also proven to be a valuable strategic tool and has broadened situational awareness across the region.

Country Profiles

This part outlines how each NB8 country counters a threat based on analytical categories. The categories were based on gathered data and the capability definition and assessment framework referred to above. It is worth noting that each country uses different conceptual terms to describe the threat and their counter-activities. In this report we have used the term IIO to describe the phenomenon. However, in cases where we refer to an individual country's approach, we use their term.

Denmark

Denmark, a Nordic country with a population of close to 6 million, is a founding member of NATO and joined the European Union in 1973. Denmark has progressively acknowledged the threat posed by IIOs to the state, though it has not yet experienced any coordinated campaigns comparable to those initiated against Baltic countries. While debates about civilian defence have resonated historically in Sweden, Denmark has in contrast approached these questions in recent years with a stronger security and intelligence-based focus. This sees the primary work on responding to external threats against Danish national interests undertaken by a discreet expert task force, while more well-established broader societal and civilian defence issues remain in the early stages of coordination.

Framework and structure

The Danish government established Task Force Interference in 2017 as an inter-ministerial task force to coordinate Danish efforts against state-sponsored external IIOs, and ensure state authorities responded to incidents effectively. The Task Force serves as the primary coordinating mechanism for Denmark, Greenland, and the Faroe Islands, with representation from the Ministry of Justice, Ministry of Foreign Affairs, Ministry of Defence, Ministry of Resilience and Preparedness, Danish Resilience Agency, Danish Defence Intelligence Service (DDIS), and Danish Security and Intelligence Service (DSIS). The focus of the Task Force centres on monitoring and countering foreign IIOs and also convenes to assist with special events, such as elections. The current legislative framework was amended in 2019 to criminalise foreign IIOs under Section 108 of the Danish Criminal Code. Denmark uses the term 'illegal influence' to define this practice, identifying it as cooperation with a foreign intelligence service on influence activities aimed at affecting decision-making or influencing public opinion, which encompasses both overt and covert action.

Denmark has a comprehensive approach, encompassing legal, diplomatic, political, intelligence, and resilience aspects in responding to IIOs. The inclusion of representatives from Greenland and the Faroe Islands is also significant, reflecting an awareness of regional vulnerabilities and the need for fully inclusive security strategies. Denmark strongly supports coordinated responses between countries and actively engages in regional frameworks, in particular those instituted by the EU and NATO.

Countering the threat

Resilience building is an important element informing Denmark's approach to countering IIOs, primarily led by the Ministry of Digital Affairs and the Ministry of Culture. This focus reflects an understanding that long-term resistance to IIOs requires empowering citizens with critical thinking skills and media literacy. The Ministry of Digital Affairs has a dedicated department focusing on social media, tech, and democracy, specifically tasked with monitoring the effects of tech giants on democracy, social cohesion, and the well-being of children. As a reliable and independent media has a crucial role in ensuring democratic resilience as a counterweight to IIOs, the Ministry of Culture supports the ongoing development of a robust and impartial media sector via an active media policy. The Ministry of Culture has departmental responsibility for the media sector, including the Danish public service broadcaster and a number of funding schemes allocated for the private media sector. Additionally, the Danish Resilience Agency (SAMSIK) also participates in Task Force Interference. In the current version of the Danish *National Risk Profile (Nationalt Risikobillede, NRB*, 2025, published by SAMSIK), IIO, disinformation, and misinformation are identified as risks to societal cohesion.

This departmental structure is significant as it positions resilience building as a distinct function separate from the immediate security-focused work of the Task Force. The Ministry of Digital Affairs and Ministry of Culture are not currently represented within the Task Force structure, demonstrating a clear distinction between the security dimension and strategies for fostering democracy.

Strategic communication is an evolving capability within Denmark's foreign influence response framework. The Ministry of Foreign Affairs currently monitors disinformation in the context of international media, leveraging input from its embassies and their active participation within international forums such as the EU RAS and NB8. Furthermore, the two Danish intelligence agencies – DSIS and DDIS – play a crucial role in strategic communication efforts through assessments, attribution, and public statements. Generally, these assessments have not indicated the presence of any imminent, large-scale coordinated attacks akin to those seen in the US or France. Instead, the primary concern revolves around smaller, faster, and more opportunistic IIOs designed to sow discord, undermine trust in institutions, and potentially impact public opinion during key political processes, such as general elections or elections for the European Parliament. More recently the political situation concerning Greenland has prompted both the DSIS and DDIS to identify these conditions as a potential opportunity for foreign actors to engage in IIOs. The intelligence agencies have also detected an IIO where fake profiles of Danish and Greenlandic politicians were used as part of a broader disinformation campaign during the 2025 Greenlandic election.

In the unclassified assessments released by the Danish intelligence agencies, Russia is identified as the most likely perpetrator, leveraging its significant resources and established capacity for engaging in IIOs. Its motivation is not necessarily to directly alter election outcomes, but rather to create societal fragmentation and weaken support for EU policies, in particular those relating to sanctions against Russia and support for Ukraine. China's potential involvement is also noted, though it is considered to be a less immediate threat in terms of direct electoral interference. Public statements by the intelligence agencies have identified Denmark's election infrastructure as being robust and, most importantly, difficult to hack.

In general, Denmark is a strong advocate for coordinated international efforts in countering IIOs, particularly within the EU and NATO. Public authorities have frequent dialogue with social media companies, including through diplomatic representation in Silicon Valley and a dedicated global tech ambassador.

Conclusion

Denmark's approach towards IIOs is characterised by close inter-agency collaboration and an established legislative framework to tackle 'illegal influence'. Intelligence agencies play a key role in this approach. In addition to Task Force Interference, there is ongoing work focusing on societal resilience and in building strong partnerships across society.

Estonia

Estonia, a Baltic country with a population of under one and a half million, restored its independence in 1991. In 2004 it became a member of the EU and joined NATO, and since 2008 the NATO Cooperative Cyber Defence Centre of Excellence has been based in the capital, Tallinn. The country has been a persistent target for IIOs, which have largely been attributed to the Russian Federation. The 2007 hybrid attack on Estonia acted as a catalyst for substantive change in its strategic approach, placing it at the forefront of understanding those tactics which inform contemporary IIOs. As a small, well-networked digital society, Estonia remains resilient to IIOs. However, the combined effects of ongoing geopolitical instability and societal polarisation within Estonia require a heightened state of awareness and a whole-of-society approach to effectively counter the threats posed by IIOs.

Framework and structure

The National Security Concept of Estonia (NSC, 2023) provides an overview of the Estonian security environment, and functions as a framework document for sector-specific strategies and development plans in responding to security threats. Strategic communication is singled out as a key approach in ensuring that constitutional values are embraced as widely as possible in society. Such a strategy has been implemented as a preventive measure against IIOs which may lead to conflicts which threaten the constitutional order. The role of strategic communication is further reinforced in Estonia's strategic approach via the National Defence Development Plan (NDDP, 2022–2031), which identifies strategic communication as one of five pillars of national defence.

The NSC identifies societal cohesion and collective resilience as core elements in resisting IIOs. Key aspects of this approach include citizen trust in the state, a strong and robust civil society, risk awareness, defence resolve, and readiness to volunteer for crisis resolution. In addition, international cooperation (NATO, EU, and Baltic Sea region formats) is seen as instrumental in strengthening Estonia's security and resilience capabilities.

The Strategic Communications Department of the Government Office is the lead actor responsible for the coordination and implementation of state strategies in cooperation with other state institutions and partners. A Strategic Communications Council operates under the Government's Security Committee, involving the Government Office, Ministry of Defence (including the Estonian Defence Forces), Ministry of Internal Affairs, Ministry of Foreign Affairs, security services, and other agencies as required. The Council convenes weekly meetings to exchange information and discuss different courses of action. Estonia's key public actors are shown in Table 2.

Government Office (Strategic Communications Department):

- Lead coordinator for Strategic Communication.
- Monitors social media activity.
- Undertakes surveys on attitudes.
- Develops policy on media literacy.
- Plans crisis communication.

Ministry of Foreign Affairs:

- Engages in international strategic communications networks and organisations.
- Helps disseminate messages important for Estonia through its networks, including embassies.

Ministry of Defence:

- Coordinates the strategic communications of the defence sector.
- Conducts annual polling on attitudes.
- Works closely with the media sector and partners on awareness raising.

Estonian Defence Forces:

- Monitors the information environment and shares analytical products with other public actors.
- Regularly polls public opinion.
- Provides internal StratCom training.

Estonian Internal Security Service (KAPO):

- Monitors information environment.
- Communicates to the public on IIOs.
- Conducts proactive media briefs.
- Initiates legal action against unlawful IIOs.

Consumer Protection and Technical Regulatory Authority:

- Mandated agency responsible for limiting hostile foreign media broadcasts.

Ministry of Education and Research:

- In cooperation with the Government Office, develops and implements media literacy policy and the National Media Literacy Action Plan.

TABLE 2. Estonia's key public actors

Internationally, Estonia takes part in various EU and NATO formats, namely the EU RAS and NATO RRG. Participation in these entities has an important function for joint awareness-raising and better-coordinated responses. There is a daily information exchange with Estonia's closest allies – Latvia, Lithuania, Finland, the UK (lead for the NATO multinational battalion battle group based in Estonia), and France (part of the multinational battalion battle group). Regular information exchanges with other Allied countries assists in avoiding conflicting messaging, as well as increasing knowledge and understanding of one another's activities.

Countering the threat

The NDDP prioritises situational awareness through monitoring both domestic and international media sources, as well as undertaking regular public opinion surveys to gauge public attitudes in Estonia. The Strategic Communications Department of the Government Office commissions a quarterly public opinion survey and a large-scale biannual survey. The Department also monitors social media discourse. The information space is scrutinised to identify any hostile IIO and evaluate any potential impact. In this context the Analytical Department of the Estonian Defence Forces and state security services, namely KAPO, both complement the monitoring work of the Strategic Communications Department of the Government Office.

Representatives from both KAPO and the Estonian Defence Forces participate in the weekly meetings of the Strategic Communications Council, sharing observations and receiving information for further evaluation. The Analytical Department and Public Affairs branch of the Estonian Defence Forces actively engage in detecting hostile IIOs. Defence Force personnel regularly receive training provided by the Estonian Defence Forces' StratCom Centre to ensure members can undertake monitoring activities. Estonian Defence Force units focus on monitoring narrower information channels and other sources not covered by the Government Office's Strategic Communications Department, and will issue early warnings to relevant actors if deemed appropriate.

Resilience is built on a whole-of-society approach, encompassing state agencies, the media sector, civil society, businesses, and residents of Estonia. In a small and well-networked society, such as in Estonia, resilience is strengthened by overlapping membership of individuals and institutions in various formats. Government, media, business, and civil society actors, for example, engage with one another via their participation in the Defence League, a voluntary national defence organisation administered by the Ministry of Defence. Additionally, several civil society actors, such as Propastop, play a key role in countering IIOs. Government agencies also cooperate with some civil society organisations as part of their public outreach efforts. These include government grant schemes for small-scale projects or offering their own expertise to assist civil society organisations on projects which facilitate public engagement on state security and foreign policy issues. Estonia also prioritises language education as a resilience measure to protect its information environment against IIOs. In late 2022, for example, Estonia passed an education reform bill requiring the full transition of all schools to Estonian language instruction by 2030.

Media literacy is a core component in Estonia's work to counter IIOs. It is being integrated into education and adult retraining programmes, supported by well-trained professionals, educators, and community activists specialising in both information threats and societal resilience. Estonia is among the highest-ranking countries listed in the Media Literacy Index, though assessing media literacy levels remains a challenge. Furthermore, the Government's Strategic Communications Department collaborates with the Ministry of Education and Research on media literacy policy and the National Media Literacy Action Plan. Focus areas include integrating media literacy into school curricula, public awareness campaigns, and strengthening networks. The two institutions also coordinate a Media Literacy Network, which consists of 30 members and includes representatives from civil society organisations, media organisations, the Ministry of Culture, the Estonian Police and Border Guard, and the national public broadcaster, ERR.

Since the full-scale invasion of Ukraine in 2022, public perceptions of intelligence agencies have changed due to their increased media presence in Estonia. Weekly press conferences are organised by the Ministry

of Defence, providing public information on Russian activities in Ukraine using Estonian military intelligence. In addition, KAPO and the Estonian Foreign Intelligence Service both publish detailed annual reports and maintain an open communication with the media sector to build threat awareness among the public.

The Department of the Government Office defines strategic communications as 'planning and integrating the activities of the state into a coherent communicative whole and communicating it to society'. Effective government strategic communications, alongside a competent media and strong civil society, are seen as the best preventive measures to deter and undermine IIOs.

In regard to direct responses, overall resilience and pre-emptive communication of Estonia's own story is given higher priority over a case-by-case response strategy. Direct rebuttal is only done by state institutions when incidents are considered time critical or when their potential impact is assessed to be sufficiently critical. Otherwise media and civil society organisations work proactively to verify and debunk disinformation, as well as investigating foreign influence attempts.

For increased crisis management capacity, the Government's Strategic Communications Department has established a Communications Reserve. The Reserve consists of around 100 specialists from other government agencies, media, civil society, and the private sector, who can be mobilised to assist in a crisis response. Communication Reserve representatives participate in regular training exercises to ensure they are able to respond whenever required. Each government agency is responsible for managing its own crisis communication, including responses in relation to any detected incidents. The Government Office will assume control of any response if the situation escalates to become a national crisis.

A number of legislative measures have also been implemented to specifically limit Russian IIOs:

- Following the full-scale invasion of Ukraine, Estonia enforced EU-wide broadcasting sanctions against Russia.[3]

- In 2025, in response to the Russian Orthodox Church's support for Russia's war against Ukraine, the Estonian Parliament passed a law stipulating the separation of the Orthodox Church of Estonia from the Moscow Patriarchate, and made the right to vote in municipal elections a prerequisite for membership of the clergy.

- In 2025 another bill was introduced in the Estonian Parliament granting the Consumer Protection and Technical Regulatory Authority powers to limit the broadcasting of hostile foreign media services. While broadly seen as a means to counter Russian and Belarusian disinformation, the scope of the legislation technically extends to any third country (non-EU countries) operating in Estonia.

3 The percentage of Russian speakers naming Kremlin-controlled channels among the top three most important sources of information declined from 37 to 19 per cent in early 2022, and further to 11 per cent by early 2023. See: 'Survey: Kremlin channels lose significance with Russian-speakers in Estonia', *EER*, 12 April 2022, *https://news.err.ee/1608562720/survey-kremlin-channels-lose-significance-with-russian-speakers-in-estonia*. Joakim Klementi, 'Russian info channels in Estonia viewed, trusted far less than a year ago', *EER*, 9 March 2023, *https://news.err.ee/1608909242/russian-info-channels-in-estonia-viewed-trusted-far-less-than-year-ago*.

Conclusion

The Estonian approach to countering IIOs is characterised by proactive strategic communications, close collaboration between relevant agencies, a distinct media literacy programme, an active intelligence service, and a legislative toolbox for disrupting foreign influence.

Key takeaways

- Media literacy, awareness raising, Estonian language instruction, and ensuring alignment with Estonian constitutional values are a priority for the Estonian government in mitigating the impact of IIOs.
- Legislative and regulatory initiatives are common tools of Estonia's approach, with the intent of limiting the visibility and spread of IIOs.
- Openness and strategic messaging of the Estonian intelligence services raise public awareness of known threats against the country and signal deterrence.
- A central hub – the StratCom function of the Government Office and the Strategic Communications Council – coordinates state responses in countering IIOs.

Finland

Finland, a Nordic country with a population of around 5.6 million, shares a long border with the Russian Federation and has a history of navigating complex geopolitical dynamics. It became a member of the European Union in 1995 and joined NATO in 2023. Finland has consistently ranked among the top countries in global education, governance, and press freedom. Furthermore, it has a strong tradition of media literacy, national preparedness, and a whole-of-society approach to security, which creates a strong foundation for countering IIOs. However, the evolving global security environment may create challenges in safeguarding societal resilience.

Framework and structure

The Finnish approach to countering IIOs is informed by its 'Comprehensive Security Framework' – a model based on the idea that the vital functions of society are safeguarded via collaboration between state authorities, the business community, organisations, and citizens. Thus, the framework has a broad approach and is not specifically focused on countering IIOs.

The *Security Strategy for Society* (2025) is the most important directive document informing the Finnish model of comprehensive security. In this context each citizen is perceived as a security actor and has a responsibility in ensuring societal resilience. This strategy also established the principles and responsibilities of relevant state authorities/agencies in safeguarding the vital functions of society, identifying 'strategic tasks' and clearly

defining the roles assumed by each institution in this context.

The strategy acknowledges the role of 'systematic and goal-oriented strategic communication based on the analysis of the information environment' in strengthening societal resilience against IIOs. The strategy highlights that 'preparedness for and response to IIO relies on close collaboration between authorities and key stakeholders. During prolonged crises and disruptions, communication efforts are supported by shared or individual contingency plans, as well as special operating models. Readiness for communications in disruptions is developed through joint training and exercises.'

According to the latest *National Risk Assessment* (2023), IIOs are identified as one of the key threats to Finnish society and would have a significant impact on all vital functions of society. To date, this threat has not had any extensive or paralysing effects on the operational capacity of the Finnish state, possibly due to the fact that Finland is not considered to be a primary target of IIOs by hostile actors.

The responsibility of countering IIOs is shared between different governmental institutions whose roles are defined by the applicable legislation. This means that if one particular sector is targeted (e.g. agriculture), the relevant ministry will be responsible for managing its response to the incident, and other state institutions would only function in a supporting capacity.

The Prime Minister's Office also has a coordination role when it comes to official strategic communication. For example, the Office administers a number of forums to facilitate engagement, including an informal cross-governmental network of communicators. This entity combines representatives from state authorities, including ministries, government agencies, and others. The Office also holds frequent meetings with the communication directors for all government ministries. In crisis conditions the Government Communication Department may also assume a leadership role, subject to decisions of government plenary sessions.

As part of the Project for Developing the Government's Security Management Framework, the role and model of strategic communication at the governmental level are being updated and enhanced.

Finland's key public actors are shown in Table 3.

On an international level, Finland participates in most of the current multilateral cooperation formats. The EU RAS and NATO RRG formats are considered to be the most important frameworks within the region.

Prime Minister´s Office, StratCom Team:

- Develops and leads the coordination of national strategic communications.
- Contributes to awareness raising through public threat reports.
- Collaborates with government agencies, NGOs, and the media to build resilience.

Ministry of Foreign Affairs:

- In cooperation with the Prime Minister's Office and other ministries, plans and implements strategic communications relating to foreign and security policy.
- Cooperates with foreign partners.
- Engages in public diplomacy efforts.

Ministry of Defence:

- Conducts daily media monitoring.
- Provides information environment analysis on defence-specific topics.

Defence Forces:

- Has responsibility for national military strategic communications.
- Conducts weekly information environment analysis, which is shared with other state actors.
- Conducts national defence courses and supports the organisation of regional defence courses.
- Raises awareness on comprehensive security, total defence, and military capabilities to defend the country.

Finnish Security and Intelligence Service (SUPO):

- Raises awareness of threats to society through public communication efforts.
- Gathers intelligence on potential threats to national security in the information environment and acts to counter them.

Finnish Transport and Communications Authority (TRAFICOM):

- National information security authority.
- Monitors and analyses emerging threats in the information environment when they are linked to cybersecurity.
- Provides guidance and support to public authorities, NGOs, businesses, government leadership, and citizens on how to identify and respond to cyber threats (including IIOs).
- Implements and supervises implementation of the Digital Services Act in Finland.

National Emergency Supply Agency (NESA):

- Conducts information environment analysis.
- Coordinates engagements with the business sector.
- Organises training exercises.

TABLE 3. Finland's key public actors

Additionally, Finnish experts participate in both the Ukraine Communications Group and NATO StratCom COE. The European Centre of Excellence for Countering Hybrid Threats is based in Helsinki. Various international bilateral contacts are also maintained by state institutions.

Countering the threat

There are several state actors conducting some form of information environment analysis in Finland. The Prime Minister's Office centres its activities on hostile influence and psychological resilience, whereas the Defence Forces and intelligence services provide threat analysis. The Finnish National Emergency Supply Agency (NESA) has developed online information environment analysis capabilities, with the focus on developing analytical tools and models which can assist other institutions.

The different analysis aims to assess informational threats as well as psychological resilience. The Prime Minister's Office regularly cooperates with NGOs and academic institutions in developing public communication tools to strengthen psychological resilience. Measurements include, for example, an assessment of citizen trust in democratic institutions, undertaken in Finland four times a year.

The Security Strategy for Society highlights psychological resilience as one of seven vital functions of society. Finland has identified mutual trust, awareness raising, and public confidence in authorities as essential pillars of psychological resilience, making the credibility of state institutions and the services they deliver critically important to uphold.

Raising awareness on potential threats is a key focus area in strengthening the psychological resilience of the population. With the aim of educating society and deepening understanding of information influence, the Prime Minister´s Office published the first public overview of information influence activities in January 2025. The overview is publicly available via the website of the Prime Minister´s Office and will be updated annually. Another actor which raises threat awareness within Finland is the Finnish Security and Intelligence Service (SUPO). This has a high degree of visibility in Finland via dedicated public engagement, including the annual release of the National Security Overview and other forms of public communication outreach. Additionally, the Finnish Transport and Communications Authority (TRAFICOM) has undertaken several activities to raise public awareness on IIOs in the cyber domain. Such efforts include a weekly review by the National Cyber Security Centre Finland (NCSC-FI) and its 'Information Security Now!' online news series, available via the NCSC-FI webpage.

Regular training and exercises are organised by several actors, including the Prime Minister's Office nationally and the Regional State Administrative Agency at a regional level, to increase capabilities for countering IIOs. Several of these exercises are organised in cooperation with private companies and universities. For example, the Prime Minister's Office in cooperation with the University of Jyväskylä developed a publicly available online training course on information threats and geopolitics. Finland also offers national defence courses developed by the Defence Forces, providing an overview of the country's foreign, security, and defence policy. These courses are a long-standing feature of Finland's national defence strategy, having been organised at both a national and regional level since 1961. Such initiatives improve cooperation between different sectors of society and facilitate networking of people working in the various fields of comprehensive security.

Another actor that contributes to boosting civic preparedness capabilities is the National Defence Training Association of Finland (MPK), which offers training in different areas to support the Finnish Defence Forces, such as in countering IIOs. One example is an information influence course designed for media and communication professionals, but which is also available to the wider public.

Finland proactively engages with civil society and the private sector as part of its preparedness regime. This is administered via a pool system, led and funded by NESA. The media sector is involved in this framework, encompassing all critical industry players to ensure public access to reliable information. The pool provides situational analysis on the Finnish media industry, produces preparedness reports, and organises meetings, training sessions, and seminars to support media preparedness. There is also ongoing cooperation between the public sector and the media where briefings are held with the media to provide context on current IIOs, and often the media sector or civil society would action a response independently.

There have been cases, however, where Finnish state institutions have initiated reactive communication measures after being targeted by manipulated content. For example, in 2022 there were videos circulating on social media where pro-Kremlin accounts claimed Finnish troops had been transferred to the Russian border. In reality, the Finnish Defence Forces were engaged in training exercises that were not even close to the border region which was being communicated. A correction request was issued by Finnish state institutions to those news outlets which were reporting on the incident to rectify the situation.

As an EU country, Finland adheres to EU sanctions on Russian state media outlets, and legal action can be taken for any breaches of these provisions by, for instance, refusing to grant a broadcast licence to any radio or TV channel contravening these measures. The government agency charged with regulating communications, TRAFICOM, is responsible for initiating any such action.

Conclusion

In conclusion, Finland's approach to countering IIOs is characterised by a whole-of-society approach to support its comprehensive security system. Finland openly communicates the threats posed by IIOs, using its own security services and cooperation with the media sector to inform and prepare its population.

Key takeaways

- The comprehensive security model, and the manner in which it is applied to build resilience and preparedness across all layers of society with the pool system, is central to Finland's strategy.
- Finland's strategy is grounded on its intention to create a resilient population via a media-literacy-focused educational system, awareness raising through communicative and engaged public institutions – namely the Office of the Prime Minister and SUPO – and recognition of psychological resilience as being fundamental to societal functions.
- Finally the informal network of coordination and information sharing is also a key characteristic of Finland's approach to countering IIOs.

Iceland

Iceland, a Nordic island country with a population of just under 400,000, is a founding member of NATO and has maintained strong transatlantic ties since the foundation of the Alliance in 1949. Although not a member of the European Union, Iceland is part of the EEA and Schengen Zone, maintaining close cooperation with European institutions. The state's security policy rests on two pillars: NATO membership and a bilateral defence agreement with the United States. While traditionally less exposed to foreign IIOs than other Nordic-Baltic countries, Iceland is not immune to such threats. Given its strategic location in the North Atlantic and proximity to the Arctic, a region increasingly targeted by hostile actors, it is anticipated that IIOs will become more commonplace.

Framework and structure

Iceland's approach to national security is guided by the *National Security Policy* (2016). The Policy encompasses global, societal, and other risks, and indicates the Icelandic

approach to foreign policy, civil security, and external defence cooperation. This document identifies both its membership of NATO and the bilateral defence agreement with the United States as fundamental components in Iceland's defence strategy. The Policy is implemented through shared ministerial responsibilities in accordance with Presidential Decree No. 6/2022 on the division of administrative affairs among ministries of the Government of Iceland.

The nation leans heavily on international strategies and NATO guidelines, and cooperates closely with international organisations and neighbouring Nordic partners. Lessons are gathered from its regional partners via lectures, training and workshops, research, cooperation, and collaboration. While the National Security Policy does not currently identify IIOs as a security issue, it does prioritise Iceland's independence, sovereignty, and democratic governance as strategic interests, and it sets out a whole-of-society approach to digital sovereignty and information security as one of its 12 strategic objectives. The National Security Council is mandated by parliamentary resolution to monitor the implementation of the Policy at a ministerial level, and functions as a consultative forum on national security issues.

With regard to domestic coordination on countering IIOs, an inter-agency Liaison Group under the National Security Council is tasked with scrutinising possible IIOs aimed at undermining trust in society and democratic values, and particularly with mapping potential manifestations and the extent of information disorder in Iceland. The group drafts proposals for projects aimed at strengthening open and informed democratic debate and democratic resilience, with the involvement of ministries, institutions, and academia. The Office of the National Police Commissioner, the Ministry for Foreign Affairs, the Electronic Communications Office, and the Icelandic Media Commission are also important actors in this context.

Iceland's key public actors are shown in Table 4.

Liaison Group under the National Security Council:

- Cross-sectoral group, consisting of actors from the Prime Minister´s Office, the Ministry of Justice, the Ministry for Foreign Affairs, the Ministry of Culture, the National Commissioner's Office of the Police, the Media Commission, academia, and the media sector.
- Tasked with scrutinising possible IIOs towards Iceland aimed at undermining trust in society and democratic values.
- Drafts project proposals to strengthen open and informed democratic debate and democratic resilience.

Ministry for Foreign Affairs:

- Has supreme authority over national defence affairs and the implementation of Defence Act No. 140/2012.
- Responsible for developing threat assessments in the field of defence, and for shaping and implementing Iceland´s security and defence policy in the international arena.
- Since 2025 has incorporated CERT-IS as the governmental cybersecurity team, which serves as the national response unit for threats, incidents, and risks in the field of cyber and information security.

Office of the National Police Commissioner:

- Coordinates approaches to various threats including natural disasters, border controls, and national security issues.
- Provides situational awareness in relation to information incidents.

Ministry of Culture, Innovation, and Higher Education:

- Focused on policy, regulatory, and educational aspects of media and information security.
- Currently drafting national media strategies, including a media policy and action plan through to 2030, which aims to strengthen journalism, media literacy, and public resilience against disinformation.

Media Commission:

- Independent public authority under the Ministry of Culture.
- Responsible for issuing broadcasting licences.
- Promotes media literacy, informing the public on disinformation.
- Conducts research on trust, media usage, polarisation, etc.

TABLE 4. Iceland's key public actors

Internationally, Iceland is a member of organisations dedicated to defence against hybrid threats, such as the European Centre for Countering Hybrid Threats, the NATO Cooperative Cyber Defence Centre of Excellence, and other multilateral cooperation frameworks. There is close cooperation between Nordic states via Iceland's involvement in the Nordic 5 and the NB8. Iceland is also engaged internationally in various networks related to media literacy and resilience, such as the European Platform of Regulatory Authorities (EPRA) Media Literacy Network (MIL).

Countering the threat

The Office of the National Police Commissioner is the main actor monitoring IIOs. However, information influence is just one of many areas the Office is responsible for, and thus it undertakes the monitoring function with limited resources. It therefore mostly relies on external tip-offs to inform its activities. The focus is on the social media environment, a field where the Office collaborates with major platforms, such as Meta. The latter has provided education and training to Office staff members and has been responsive to incidents reported by the Office as part of its monitoring function.

In building resilience, the National Civil Preparedness System has been a long-standing approach used in response to natural hazards, such as volcanic eruptions, and provides a solid foundation for resilience activities. The Department of Civil Protection and Emergency Management, which oversees the System, enjoys a high degree of public trust. However, trust in national and local governments – and in institutions such as the courts and judicial system – is generally lower in Iceland than in other Nordic countries. There is also data indicating that public acceptance of conspiracy theories relating to politics is relatively high. This relates partly to the country's experiences during the 2008 global financial crisis, which severely impacted Iceland.

Among the activities that are being conducted to enhance resilience, media literacy is given a high degree of priority. The Media Commission regularly runs a number of literacy projects, including communication and educational outreach programmes tailored to different audiences. An example of this is an educational campaign to raise awareness of risks and vulnerabilities in social media for school-age children. The Media Commission also hosts an annual media literacy week and conducts national research on media literacy levels in Iceland. There have also been

communication efforts to raise awareness on how to detect misinformation. The goal is to promote media literacy among the general public, but due to limited resources current efforts are limited. The state actively cooperates with media agencies, which also assist in amplifying communication campaigns run by the Media Commission. However, the media landscape is quite fragile and there are only a few investigative media outlets with expertise in IIOs. In terms of exercise and training, Iceland relies heavily on external support.

Iceland has so far avoided major incidents in the information domain, partly due to the relatively small number of Icelandic speakers. At the same time, the country is a frequent target in the cyber domain, mostly by actors suspected of being linked to foreign states. With the introduction of sophisticated large language models, it is now more difficult to uphold the integrity of the information environment, as several models are now well trained in the Icelandic language. There have been a few notable incidents in recent years, including false accounts mimicking those of several politicians, including the Prime Minister. These accounts were exposed and eventually taken down by the police.

As an EEA member state, the adoption of the Digital Services Act and the Digital Markets Act into Icelandic legislation is envisaged in accordance with the EEA Agreement. Additionally, while Iceland is not required to enforce the EU media sanctions introduced against Russia and Belarus, the government has aligned itself with these provisions. At the national level, a legislative act from 1978 (1978, nr. 62 20. Mai) prohibits the funding of political parties by foreign entities and the support or financing of local newspapers by foreign embassies.

Conclusion

In conclusion, Iceland's approach towards IIOs is characterised by resilience building, inter-agency collaboration, and international collaboration. The Media Commission plays a key role in educating the public, while the Liaison Group at the National Security Council represents a national centre of gravity for all IIO-countering activities. International actors contribute to professional development of the public administration given the limited resources of the country, and cooperation through, for example, participation in the NATO Cooperative Cyber Defence Centre of Excellence in Tallinn and in the European Centre of Excellence for Countering Hybrid Threats (Hybrid COE) in Helsinki has proven valuable.

Key takeaways

- Being a small country creates favourable conditions for reaching out to wider society for resilience-building purposes, and also makes cross-sectoral cooperation fast and flexible. At the same time, penetration in the domestic information environment from a hostile actor might be rapid.
- Iceland has valuable experience in building resilience against natural disasters and through those efforts an active inter-agency collaboration. This is something that could be harnessed in case of IIOs targeting the country.
- Limited resources make the state administration dependent on foreign assistance for training and education, and thus international collaboration is key for building capabilities and drawing valuable lessons.

Latvia

Latvia, a Baltic nation with a population of under 2 million, regained its independence in 1991 and joined both the European Union and NATO in 2004. It hosts the NATO Strategic Communications Centre of Excellence, established in 2014. Latvia is a long-standing target of IIOs from Russia and has been exposed due to both its geographic location and sizable Russian-speaking population. The country has taken several steps in recent years to protect itself from IIOs, including strengthening media literacy, building civic resilience, and amending its penal code to counter Russian IIOs.

Framework and structure

Securing Latvia's information environment has been identified as a strategic priority by the Latvian government in recent decades due to increasing signs of Russian efforts to use IIO to achieve its strategic objectives. Threats to the Latvian information environment were first identified as a risk in the *State Defence Concept* (2012–16) and have been included in subsequent editions.

The current *State Defence Concept* (2023–27) focuses on comprehensive defence, which is based on three pillars: resilience on an individual level, collective resilience (communities, business, municipalities), and state resilience. It identifies the need to 'enhance the resilience of government and society against various manipulations, including disinformation and information influence operations'. The *Concept* also emphasises the need to increase societal resilience and public understanding of current threats to national interests, as well as to identify the intentions of potential aggressors.

A second important document which informs Latvia´s approach to countering IIOs is the *National Concept on Strategic Communication and Security of the Information Space (2023–2027)*. The purpose of the *Concept* is to have 'a centralised model for coordination of strategic communication and security of the information space'. It is intended to promote the resilience of both Latvian public institutions and Latvian society against IIOs by strengthening the three foundations of the information space:

1. National strategic communication capabilities
2. The media environment
3. Media and information literacy.

Latvia has adopted an inter-agency approach in hostile information monitoring, detection, analysis, and response. Coordination structures have been established under the leadership of the State Chancellery's Department for Strategic Communication and Coordination, which regularly engages with other relevant institutions. The Department holds weekly meetings with communicators from relevant ministries. It also holds monthly meetings with 17 different agencies, including media regulators and security institutions which specifically focus on information security. Coordinative meetings are also held with regional actors, although with less frequency. Overall, Latvia benefits from having a relatively small government and administration; state institutions are well connected, and cooperation between these entities is rather informal and flexible, creating opportunities for rapid coordination.

Latvia's key public actors are shown in Table 5.

State Chancellery, Department for Strategic Communication and Coordination:

- Leads the coordinative work on strategic communications and information security.
- Undertakes concept development, information campaigns, and monitoring of the domestic information environment.
- Provides training and exercises contributing to building societal resilience.

Ministry of Foreign Affairs:

- Facilitates cooperation with foreign cooperation partners.
- Engages in public diplomacy efforts.

Ministry of Defence:

- Conducts resilience building including lectures, training, and exercises on civil preparedness.
- Organises public information campaigns on civil preparedness.
- Provides grants for NGOs working on societal resilience.

National Armed Forces:

- Conducts threat analysis, which is distributed to defence and state leadership and NATO partners.
- Takes part in resilience building by conducting lectures, training, and exercises relating to the state defence curriculum.

State Security Service:

- Conducts threat analysis and investigations related to the Criminal Code.
- Undertakes preventive consultations with potential perpetrators.

National Electronic Mass Media Council of Latvia (NEPLP)

- Blocks websites and restricts domains which violate national and EU sanctions.
- Conducts a media literacy programme, including hosting a media literacy database.

TABLE 5. Latvia's key public actors

In regard to cooperation with non-state actors, there are several ad hoc collaborations, although without any formalised coordination in place. State authorities maintain good relationships with a number of think tanks, such as the Baltic Centre of Media Excellence, as well as several media organisations. In terms of practical support from the Latvian state, a consistent stream of funding is distributed to NGOs working in this space. However, there is currently no overall coordination framework for all the grants being distributed, as these are administered by various state ministries.

Latvia is an active international partner and participates in several multilateral formats including the NATO Rapid Response Group, the EU RAS, the G7 Rapid Response Mechanism, and the OECD Hub on Information Integrity.

Across all three Baltic countries, there is a history of strong cooperation and informal peer-to-peer coordination formats between different government agencies and the armed forces. Similar engagement strategies have been instituted between the Baltics and important regional partners, namely Poland and Finland. With regard to the Baltic Sea region, there has been more direct cooperation and information exchange between Latvia and the Nordic countries.

Countering the threat

Regular information environment analysis and assessment, albeit with a slightly different focus, is conducted by various state institutions. Some concentrate on domestic policy issues, whereas others centre on detecting any worrying trends which may be exploited by hostile actors. Situational awareness products are distributed to key stakeholders as required.

As a consequence of the Russian invasion of Ukraine and lessons derived from the war, Latvian state institutions are now prioritising building societal resilience against the threat posed by Russia, as well as boosting civic preparedness for any potential crisis situation. For example, in 2024 national defence education became part of the mandatory curriculum in Latvian secondary schools. In addition, the Ministry of Defence is also organising regular lectures on civic preparedness in crisis situations for younger students (towards the end of primary schooling). Latvia has also reformed its educational policies, designating Latvian as the official language of instruction in all schools.

The State Chancellery provides capacity building opportunities to those involved in communication, including spokespersons and representatives from other relevant state actors. Another effort is aimed at increasing civic preparedness in the Latvian regions and municipalities, where special training is provided for communicators there. The Ministry of Defence is also conducting regular seminars within the regions, including tabletop exercises with scenarios on how to counter information attacks. Another initiative is the publication of the *Handbook Against Disinformation: Recognise and Resist* by the State Chancellery, aimed at capacity building for both civil servants and the public. The *Handbook* provides guidance on how to identify and respond to information threats.

Media literacy is also considered as an important strategy to enhance resilience. In this context several actors have assumed a significant role, though the different approaches are not determined by a national-level strategy. For example, since 2023 the National Electronic Mass Media Council of Latvia (NEPLP) has administered the 'Media Literacy Database', which functions as a repository for materials focusing on media literacy from 30 stakeholders. The NEPLP also conducts workshops for electronic mass media organisations to increase their capabilities in responding to IIOs, such as on the use of generative AI in media, the Latvian language for media, and practical aspects of hybrid war. Some of these training courses have also been made available to the public. Additionally, the State Chancellery organises an annual conference focused on strategic communications, including media literacy, and engages in various projects to boost media literacy in society, particularly within schools.

Communicative responses to IIOs are assessed on a case-by-case basis, which includes assessing when a non-response is the best response to avoid amplifying a certain campaign.

Concerning disruptive measures, Latvia has in recent years modified its legal framework to counter IIOs more effectively. This includes amendments to the Electronic Communications Law, the Electronic Mass Media Law, and the Criminal Code of Latvia. For example, several amendments to the Criminal Code were introduced at the end of 2023, including stricter penalties for providing assistance to a foreign country in activities directed against Latvia and for justification of genocide, crimes against humanity, crimes against peace, and war crimes.[4] Methods available as tools for action include:

4 More information here: 'VDD: Latvijas sabiedrība saglabā noturību pret Krievijas kara propagandu', *LV portals*, 12 March 2024, *https://lvportals.lv/norises/361294-vdd-latvijas-sabiedriba-saglaba-noturibu-pret-krievijas-kara-propagandu-2024*.

Preventive talks with a potential perpetrator (either in person or online) in order to inform/warn them that their actions may be unlawful. The aim is to deter other potential perpetrators from acting and decrease the potential tensions/conflicts in the online information environment.

Criminal investigation in case of illegal activities. One example is the case of the 'Baltic Antifascists', a Telegram channel created and administered by a group of local pro-Kremlin activists, operational since November 2022. The group was mimicking 'grassroots' activity countering 'fascistic policies by Latvian state authorities', but has been investigated on suspicion of assisting the Russian security services and raising funds to support Russia's war against Ukraine. The criminal investigation against the group (six people) is ongoing; however, some members have already fled the country.

Restricting Russian information sources that threaten national security – both on TV and online. As a result of the 2022 amendments to the Electronic Mass Media Law and the Electronic Communications Law, the ability to restrict content emanating from Kremlin-affiliated information channels has increased. More than 400 websites have been restricted to date, based on threats to national security. However, it is still possible to access the restricted Russian media – via illegal cable providers, a VPN, and social media.

Blocking social media content: in regard to cooperation with social media platforms there are established channels of communication between the platforms and relevant government ministries. However, the response from the platforms is usually slow or non-existent due to lack of appropriate policies. For instance, it took two weeks for one social media platform to remove content from an account impersonating a state official/institution.

Conclusion

In conclusion, Latvia's approach to countering IIOs is characterised by a number of efforts to enhance public resilience, the facilitation of a whole-of-society approach to defence, a broad suite of legislative devices to disrupt operations, and a culture of close and informal cooperation among state institutions.

Key takeaways

- For Latvia, one of the most important capabilities it is seeking to cultivate is the resilience of the population. To achieve this the state has instituted a number of measures, including a school curriculum on civic preparedness, a media literacy database, and ongoing efforts to enhance resilience within all levels of society.
- Flexible inter-agency collaboration is prioritised in Latvia under the direction of the State Chancellery via information sharing and coordinating communication activities.
- Legal measures play an important role in Latvia's approach, both to target Russia's proxy infrastructure and to restrict the possibility of pro-Kremlin content reaching audiences in Latvia.

Lithuania

Lithuania, a Baltic country with a population of 2.8 million, regained its independence in 1990 and joined both the European Union and NATO in 2004. As a frontline country bordering Russia and Belarus, it has long been exposed to IIOs. Lithuania focuses its approach to IIOs on building strategic communication capabilities, close coordination among public actors and civil society, and developing legislative tools to disrupt identified threats in the information environment.

Framework and structure

In the *National Security Strategy* (2021), disinformation constitutes one of the strategic threats to national security. Several objectives are outlined for how to counter it, including:

1. The development of capacities of state institutions and agencies to carry out targeted counter-disinformation activities.

2. Strengthening societal resilience, for example by investing in the education system and thereby improving critical thinking; delivering strategic communications campaigns and enhancing cooperation between the public, private, and academic sectors and NGOs.

3. Developing collaboration in international formats such as NATO, EU, and other organisations.

4. Developing innovative and technologically advanced intelligence and counter-intelligence activities.

Lithuania also has several legislative provisions in place, such as Article 19 (1) of the Law on the Provision of Information to the Public (PIP), which provides a mandate to relevant agencies to take action against media channels spreading disinformation.

In 2023 Lithuania established the National Crisis Management Centre (NCMC) to act as the lead coordinating body for national strategic communications. Reporting directly to the National Security Commission within the Office of the Prime Minister, the NCMC is responsible for communicating public responses to an IIO and minimising the harms caused by it.

NCMC leads the Strategic Communications Coordination Working Group, consisting of representatives from 11 institutions including the Lithuanian National Armed Forces, relevant ministries and agencies, state intelligence services, NGOs, and academia. The Working Group convenes on a weekly basis, but will also meet as required in response to incidents as they emerge. It functions as a network for information sharing and coordinates broader state responses in case of crisis or in response to potential informational threats. The NCMC also hosts a cross-institutional team of information environment analysts that prepares a weekly situational awareness assessment report. The NCMC also maintains several informal networks with civil society and media organisations.

Lithuania's key public actors are shown in Table 6.

Civil society is highly active and intertwined with the public sector in addressing IIOs. An important actor in this context is the Lithuanian Riflemen's Union, a voluntary paramilitary organisation which is partly integrated into the Lithuanian National Armed Forces. The Riflemen's Union has an integral role in efforts to build societal resilience, contributing to overall situational awareness as well as actively responding to IIOs.

National Crisis Management Centre (NCMC):

- Under the direction of the Prime Minister's Office.
- Leading coordinating body of national strategic communications, public responses to disinformation, and mitigation of the harm caused by it.

Ministry of Foreign Affairs:

- With the NCMC, coordinates potential counter-actions.
- Participates in international formats.
- Raises awareness among the Lithuanian diaspora.

Ministry of Defence:

- Coordinates strategic communications activities for the defence system, including providing communication guidelines.
- Administers an NGO grants programme to strengthen civil society and enhance civil resilience.
- Participates in several international collaboration frameworks.

National Armed Forces:

- Conducts regular situational awareness, educating actors (public and non-public) and society on IIOs.
- Participates in the coordination group led by the NCMC.

Mobilisation and Civil Resistance Department, Ministry of Defence:

- Aims to raise the resilience levels of the Lithuanian population for civil resistance during crises and war, including resilience building against hybrid threats.

Radio and Television Commission of Lithuania:

- Enforces measures under Article 19 (1) of the Law on the Provision of Information to the Public (PIP), including domain and IP-address blocking, demonetisation of advertising, imposition of fines, geo-blocking, and payment suspensions.

TABLE 6. Lithuania's key public actors

Lithuania also has a vast network of volunteers known as 'elves', consisting of up to 5,000 volunteers engaged in fact checking and debunking of hostile narratives, making a significant contribution to the country's overall counter-influence capabilities. In addition, both the Ministry of Defence and the Ministry of Foreign Affairs have several cooperation projects to engage civil society in countering IIOs, including grants to raise awareness about the threat from them.

As a NATO ally and an EU member state, Lithuania takes part in several international collaboration formats related to this area. This includes for example the NATO RRG, as well as ongoing close cooperation with the other Baltic countries. For instance, Baltic StratCom practitioners of the Ministry of Defence and Armed Forces engage in regular and ad hoc coordination of their responses to information incidents.

Countering the threat

Under the administration of the NCMC a number of actors, including ministries, the National Armed Forces, police, intelligence agencies, civil society, and the Radio and Television Commission of Lithuania, provide situational awareness of IIOs. The output of this collaboration is a unified assessment of the information environment, based on the DISARM Framework. This assessment report lays the foundation for potential response measures instituted by the Strategic Communications Coordination Working Group. Training is conducted on a regular basis to improve both the situational awareness and responses to it.

In Lithuania the education and resilience building of its citizens are given high priority as part of addressing IIOs. The National Armed Forces regularly provides training for government institutions, municipalities, and residents to increase awareness of IIOs. This training is sometimes conducted by the Armed Forces themselves but more frequently by NGOs. The Lithuanian Riflemen's Union and Civil Resistance Initiative (CRI), for example, frequently provide training and work with innovative educational approaches, such as game-based learning. Resilience work also extends to the Lithuanian diaspora in different countries via embassies. Additionally, the Ministry of Defence provides regular grants to civil society for strengthening NGOs and boosting citizen resilience. In 2024 the Ministry of Defence provided 600,000 EUR in project funding to NGOs.

In the context of civil defence, the Civil Resistance and Mobilisation Department under the Ministry of Defence is engaged in several work streams on resilience building. Since 2022 this work has been based on the concept of civil resistance, where the key objectives are to build resilience, civic will, and self-determination, as well as improving the skills and knowledge of the Lithuanian population in case of crisis or war. This includes courses on recognising hybrid threats and responding to disinformation.

In responding to identified IIOs, the NCMC established a response model outlining who is responsible for responding based on the severity of the threat:

- **Level 1 threat** – potential response should come from the Prime Minister or other minister.
- **Level 2 threat** – response is the responsibility of state institutions.
- **Level 3 threat** – NGO and media-based response.
- **Level 4 threat** – no direct action is taken.

The nature of the responses themselves vary on a case-by-case basis and may include actions such as establishing a counter-narrative and informing the public of hostile narratives. For example, in 2024 a hostile narrative was identified in response to the presence of German Bundeswehr units in Lithuanian territory, claiming the deployment of foreign military forces contravened the Lithuanian constitution. In response the Ministry of Defence constructed a counter-narrative via a press release quoting the Lithuanian Minister of Defence, stating 'all territories and areas with infrastructure developed for the German brigade will remain in possession of the Republic of Lithuania'.

Collaboration with the media also constitutes an important aspect of Lithuania's approach in responding to identified threats. If an IIO is exposed, representatives from state institutions may meet with journalists to provide information on any incident. The state will also provide guidance to the media on how an incident should be reported to the public. Additionally, civil society has a vital function as part of this response framework. Numerous NGOs, such as the Riflemen's Union, are actively engaged in responding to IIOs by identifying them, raising the alert, and countering the threat.

In countering IIOs Lithuania has also developed legislation to disrupt foreign operations. For instance, Article 19 (1) of the Law on PIP provides a mandate to relevant agencies to take action against any media channels found to disseminate disinformation, spread war propaganda, instigate war or hatred, or incite change to the constitutional order of the Republic of Lithuania. Following the Russian invasion of Ukraine, radio and television channels controlled or funded by Russia or Belarus have been banned from being broadcast or distributed in Lithuania. EU media sanctions imposed on RT and Sputnik have provided the state with an additional mandate to act against such IIOs. As of March 2025, hundreds of domains have been blocked under national law. According to a survey by the Lithuanian Radio and Television Commission, the number of people watching Russian TV channels dropped by half after February 2022. Regardless, citizens can still access pro-Kremlin media outlets via social media or by using VPN-services.

Conclusion

Lithuania has focused on establishing well-coordinated structures across all of society in order to bolster resilience among the population, creating a unified situational awareness, and developing strategic communications capabilities. The state has also prioritised the introduction of legislative mechanisms to disrupt Kremlin propaganda.

Key takeaways

- Civil society is highly integrated in Lithuania's approach to counter IIOs, in regard to both information sharing and countering the threat.
- Lithuania has invested resources into establishing a central entity coordinating responses to IIOs.
- Unified, cross-governmental situational awareness is a top priority for Lithuania.
- Lithuania has a broad range of legislative tools for disrupting IIOs, most notably Kremlin propaganda.

Norway

Norway, a Nordic country with a population of approximately 5.5 million, shares a long Arctic border with Russia and has historically played an active role in regional and international security cooperation. A founding member of NATO in 1949, Norway maintains close ties with both its European and transatlantic partners. Although it is not a member of the EU, the EU and Norway are generally close, with the EU being the country's most important trading partner. Norway is widely recognised for its strong democratic institutions, high levels of press freedom, and well-developed public trust in media and government. In recent years, due to the deterioration of the security situation in the region, Norway has faced similar challenges to neighbouring countries in how to protect its information environment – especially given its geostrategic position in the High North.

Framework and structure

Against the backdrop of the most severe security situation the country has faced since World War Two, the Norwegian government is strengthening efforts to increase civilian resilience and total preparedness. One of the main objectives of the state is to ensure that Norwegian society is able to withstand hybrid threats.

Following several commissions and inquiries on issues concerning roles and responsibilities in dealing with hybrid threats, Norway recently adopted a new council structure for ministries' work on preparedness planning, a new strategy on resilience against disinformation, and for the first time in history a national security strategy.

In May 2025 the Office of the Prime Minister launched the *National Security Strategy*, providing an overview of foreign, security, defence, and preparedness policy. It identifies Norway as a 'target of hostile influence operations' which constitutes a 'threat to trust and public debate in society'. Furthermore, it outlines the enhanced resilience of Norwegian society as one of the main strategic priorities, with prevention of, detection of, and response to hostile activities below the threshold of an armed attack being key.

The strategy for building resilience against disinformation was launched in June 2025 and points out five central areas: (1) strengthening media literacy; (2) holding social media platforms accountable; (3) supporting editorial media; (4) strengthening knowledge and research; and (5) coordination for improvement. The strategy also identifies the roles and responsibilities of different actors in Norway.

The current Norwegian structure is based upon the principles of responsibility and cooperation, making it the responsibility of the individual organisation and sector to counter any IIO targeting it. To support these actors, the Ministry of Justice and Public Security coordinates public security and emergency preparedness where IIOs are part of the picture, although this only constitutes a fraction of its overall coordinative mandate.

Norway's key public actors are shown in Table 7.

Ministry of Justice and Public Security:

- Responsible for coordinating measures against IIOs.

Ministry of Culture and Equality:

- Tasked with building public resilience towards disinformation.
- Includes strengthening pre-emptive work.
- Contributes to enhanced coordination among relevant actors.

Ministry of Foreign Affairs:

- Responsible for diplomatic, foreign, and security policy aspects of IIOs.
- Participates in international forums to facilitate information sharing.
- Provides guidance to Norwegian foreign missions on how to detect IIOs against Norwegian interests abroad.

Ministry of Defence:

- Responsible for the implementation and formulation of Norwegian security and policy (including information threats).
- Coordinates strategic communications in the defence sector, as well as international defence cooperation.

Armed Forces:

- Responsible for responding to IIOs targeting the defence sector.
- Conducts information environment assessment concerning the military.

Ministry of Local Government and Regional Development:

- Responsible for countering IIOs during elections.

Norwegian Police Security Service (PST):

- Monitors and prevents threats to national security.
- Provides support in decision-making in regard to the sovereignty, territorial integrity, and other national security interests of Norway.

Norwegian Media Authority:

- Contributes to fostering media literacy among the public.
- Will analyse and document social media platforms' policies regarding coordinated inauthentic behaviour and their compliance with the Digital Services Act.

National Security Authority (NSM):

- Conducts vulnerability analysis.
- Provides recommendations for strengthening resilience within the frame of the National Security Act.

TABLE 7. Norway's key public actors

To facilitate coordination between these different actors there are several informal networks. At the ministerial level, this includes a network on hybrid threats led by the Ministry of Justice and Public Security aimed at increasing situational awareness and sharing information. There is also close cooperation between the communications directors for relevant ministries and the Armed Forces.

At agency level, the National Intelligence and Security Centre (NESS) functions as a coordination hub for four state agencies: the Norwegian Intelligence Service (NIS), the Norwegian Police Security Service (PST), the National Security Authority (NSM), and the Norwegian Police. They work together to strengthen the national capability to identify, build understanding of, and provide decision-making support related to hybrid threats including IIOs.

Internationally, Norway participates in several networks to strengthen their capacities to respond to IIOs – primarily to share and receive information on current events, trends, and countermeasures against IIOs. These networks include the NATO RRG and the European Centre of Excellence for Countering Hybrid Threats. Norway is also the Chair of the Group of Friends of the Council of Europe on the Safety of Journalists and Media Freedom for the 2025–26 period, which focuses on disinformation and contributes to the RESIST project on Strengthening Societal Resilience to Disinformation in Europe. Norway is also in the process of joining the NATO StratCom Centre of Excellence.

Countering the threat

The PST is responsible for internal threat assessments, while the NIS monitors external threats. These are the two main actors providing situational awareness for a broad variety of threats, including IIOs. The NSM closely collaborates with the PST and NIS, complementing them through analysing domestic vulnerabilities and providing recommendations for risk reduction. The PST has recently received an increased mandate on data collection for intelligence purposes, as the agency can now systematise and analyse larger amounts of open information than had previously been allowed.

The Norwegian Armed Forces also undertake weekly information environment assessments in relation to defence issues. They also assess public perceptions of the Armed Forces, including reactions to their communication activities.

When it comes to resilience building, the NSM is a key actor operating within the frame of the National Security Act. The agency is responsible for providing information, advice, and guidance to ensure that actors take the necessary steps to protect themselves against threats, including IIOs. However, it is worth noting that the latter constitute only a small part of resilience building, and other areas, such as cyber, are the primary focus for the agency.

The Norwegian Media Authority is also an important actor in the context of building public resilience by fostering enhanced media literacy and critical thinking. Within civil society the NGO Faktisk, for example, provides schools countrywide with educational programmes, courses, and lectures on media literacy and critical thinking through their organisation Tenk, with the financial support of the Ministry of Culture and Equality. Also, through their annual national threat reports the intelligence services, PST, and NIS contribute to efforts to increase IIO-threat perception among the public. In general, it is worth noting that the Norwegian population has high trust in institutions, which provides a potential good baseline for resisting influence activities from foreign powers.

There have been cases of IIOs directed at Norway. For instance, a recurring disinformation campaign targeted the Child Protection Agency, Barnevernet, where narratives on alleged child kidnappings and religious prosecution led to worsening bilateral relations with a number of countries. The government's response ranged from strategic communications, including debunking, to diplomatic activities and strengthening bilateral cooperation between child welfare professionals through the EEA and Norway Grants. Other cases have involved for example Iran, which in 2023, through a cyber-actor with ties to the country's intelligence services, conducted a hack and leak operation at a Swedish company offering text messages. The actor subsequently sent text messages to young Muslims in Norway, urging them to avenge Koran burnings. There have also been cases of Russian rhetorical questioning of the legitimacy of the Norwegian government's policy related to military preparedness in Norway's Arctic territories, including Svalbard.

In the 2025 threat report released by the PST, the agency expects that authoritarian states will continue to engage in IIOs targeting Norway. The agency highlights for example hybrid actions such as sabotage and cyberattacks as having the purpose of achieving an effect in the cognitive space – for example, to create unrest in society or undermine confidence in societal institutions, and to weaken support for Ukraine.

Should an IIO be detected, relevant ministries, most notably the Ministry of Foreign Affairs, Ministry of Defence, and Ministry of Justice and Public Security, would choose relevant response measures considering the specific case. In that process, close collaboration and information sharing with international

partners would be a priority. Attribution by state officials has traditionally been rare for IIOs, although past events have been attributed to Russia and China in the intelligence services' public national threat assessments. For instance, the 2025 PST assessment points to an event in 2023 where for the first time a Chinese influence campaign was detected involving fake websites.

On social media the government is directly involved in debunking misinformation and disinformation in the comments sections of its social media accounts. Fact-checking organisations, such as Faktisk also contribute by responding directly to disinformation by debunking.

Legal action against IIOs may also be initiated against domestic actors if the PST finds they acted on behalf of or in collusion with a foreign intelligence service pursuing activities aimed at influencing decision-making or the formation of public opinion.

Conclusion

As with the other countries in the region, there is a high degree of connectivity between civil servants and decision-makers in Norway, with close contacts between ministries facilitating agile responses when facing threats. Several structural changes are currently on the way, making Norway an interesting case to follow during the coming years.

Key takeaways

- Like Sweden and Finland, the Norwegian approach to countering IIOs is characterised by a decentralised approach, based on the principles of responsibility and close coordination.
- The current framework is undergoing multiple changes that may affect the country's approach in the coming years.
- Close collaboration with international partners is deemed important should a direct response against an IIO take place.

Sweden

Sweden, a Nordic country with a population of over 10 million, is a long-standing member of the European Union and joined NATO in 2024. The country has a long history of addressing foreign influence as part of the concepts of psychological and total defence. In recent years the country has increased its efforts to address IIOs as part of a whole-of-society approach, whereby both the state and citizens have a role in countering such threats. However, attempts to undermine public trust in democratic institutions have increased, as Russia and actors in the Middle East have initiated interference campaigns against Sweden, and the state is now seeking to enhance its ability to address emerging geopolitical and security challenges in the region.

Framework and structure

The *National Security Strategy* (2024) serves as the overarching framework informing Sweden's work on IIOs. The strategy identifies IIOs by hostile foreign actors as a concern connected to a broader deterioration of the geopolitical and security landscape of the region.

At the government level, coordination of national security issues is managed by the Prime Minister's Office at the Organization of the National Security Adviser. The Government Offices have multiple levels of preparedness functions; in the event of a crisis, ministries receive and distribute official notifications, alert those affected within their respective ministries, summon staff members to manage the situation, and cooperate with authorities within the ministry's area of responsibility.

While the government is responsible for policy setting and overall strategy, the execution of these policies is largely delegated to semi-autonomous state agencies. While the government will issue state agencies with annual instruction letters as well as specific assignments, the Swedish system is specifically designed to minimise ministerial oversight. This has both advantages and disadvantages in addressing complex threats like IIOs. In distinction to hierarchical government structures, the agency with primary responsibility for a specific policy or social area also has responsibility for managing the response to IIO incidents.

Improving and restructuring Sweden's overall total defence assets has been identified as a key political priority. As part of this, in 2022 the Psychological Defence Agency (MPF) was established with responsibility to lead efforts to coordinate and develop operations of agencies and other actors within Sweden's psychological defence. This includes identifying, analysing, and providing support to counter malign influence activities targeting Sweden. To facilitate the work of the MPF, two cooperative councils were established: a capability-building forum and an operational forum. Meetings take place at both a director-general level and operational level to enable effective coordination. However, as each actor is responsible for managing its own response planning and capability building, this process is very resource intensive.

Sweden's key public actors are shown in Table 8.

Internationally, Sweden is active in multiple forums, including the NATO RRG, the EU RAS, the G7 Rapid Response Mechanism, the European Centre of Excellence for Countering Hybrid Threats, and the NATO StratCom Centre of Excellence.

The Prime Minister´s Office:

- Coordinates national security issues at the Government Offices.
- Leads the National Security Council, established to exchange information and provide strategic coordination on security issues. The Council is assisted by the National Security Advisor, who is responsible for analysis and coordination of national security issues.
- As part of the National Security Advisor's Organisation, the Crisis Management Coordination Secretariat conducts 24/7 monitoring where IIOs are one of multiple potential crises the office is looking into. It also coordinates relevant ministries, informs the political leadership of trends potentially triggering a national crisis, and coordinates joint preparedness exercises.

Ministry of Foreign Affairs:

- Security Policy Department manages hybrid threats, particularly from an EU/NATO perspective. The Communications Department is responsible for detecting and countering foreign information manipulation and interference (FIMI) in particular through communication, and as well as participating in several international networks and forums.

Ministry of Defence:

- Responsible for total defence (civil and military defence).
- With its underlying agencies (such as the Armed Forces, MPF, Swedish Civil Contingencies Agency – see below – and the foreign intel agencies) has a wide set of responsibilities in terms of detecting, resisting, and responding to hybrid threats.
- Also has a specific department for cyber- and hybrid affairs which cooperates closely with several other ministries.

Psychological Defence Agency (MPF):

- Central actor leading the coordination of Sweden's psychological defence.
- Monitors and analyses foreign actors' activities against Sweden, as well as focusing on bolstering societal resilience through awareness raising, capability building, and providing support to other agencies. Does not typically engage in direct public communication regarding specific actions, but rather offers guidance and resources to those responsible for handling IIOs within their respective areas.
- Role is primarily supportive, aiming to reduce the burden on frontline actors by providing information and expertise.

Swedish Armed Forces:

- Main task is to defend Sweden and its allies against an armed attack.
- Deems the information environment a vital part of military operations.

Swedish Security Service (SÄPO):

- Involved through its mandate to monitor and reduce threats to national security, including those originating from domestic threats as well as foreign IIOs.

Swedish Civil Contingencies Agency (MSB):

- As of 1 January 2026, the Civil Defence and Resilience Agency.
- Responsible for coordinating efforts within civil defence (in which psychological defence is a part).
- Manages sectoral meeting forums and coordinates crisis management.

Swedish Institute:

- Plays a role in monitoring the international perception of Sweden and providing digital tools for tracking disinformation narratives.
- Monitors the information environment in 53 languages.

Swedish Media Agency:

- Coordinates efforts on media literacy.
- Provides permits and licences for radio and TV broadcasts.
- Promotes awareness for youth and children concerning media habits.

TABLE 8. Sweden's key public actors

Countering the threat

Several actors contribute to an overall situational awareness with slightly different focus. The intelligence agencies work closely to identify and reduce the impact of IIOs, for example by maintaining an overview of the influence threats posed by foreign actors. The MPF monitors foreign actors' malign IIOs targeting Sweden, with a focus on narratives. The Swedish Armed Forces also monitors IIOs as part of its broader national and regional defence capabilities. The Swedish Institute monitors international perceptions of Sweden. The Crisis Management Coordination Secretariat within the Prime Minister's Office undertakes 24/7 situational awareness monitoring concerning potential crisis events.

One pillar of the Swedish strategy is based on enhancing societal resilience through media literacy initiatives and fostering critical thinking skills among citizens. This approach acknowledges that combating IIOs requires empowering individuals to sufficiently understand the media landscape to distinguish different sources and content, rather than rely solely on government intervention. The MPF and the Swedish Media Agency collaborate with a network of public and private actors to develop resources and provide training programmes aimed at increasing public awareness of manipulative techniques. In 2023 the MPF initiated the 'Don't Be Fooled' communication campaign, which included a handbook to help citizens recognise and deal with disinformation, misleading information, and propaganda. Another example is the *In Case of Crisis or War* leaflet developed by the Swedish Civil Contingencies Agency, as the lead state actor for civil defence, advising citizens on how to prepare for a potential war or crisis. The most recent edition of the leaflet (2024) included advice on dealing with disinformation and propaganda.

The 'given responsibility principle' dictates which agencies take the lead in managing responses to IIOs, and the MPF provides support to the responsible agency, offering guidance on communication strategies and providing contextual information. It also assists in information gathering on any identifiable actors. The MPF may also provide direct support to media outlets seeking accurate information in response to any incidents if requested.

For large-scale IIOs, government representatives have in recent years countered these through strategic communication. The state response to the LVU (the Care of Young Persons (Special Provisions) Act) campaign, an IIO targeting Swedish social services, for example resulted in the Prime Minister addressing the incident in press conferences and through the media. The Minister of Civil Defence, who also acts as a state spokesperson for the government on disinformation, has addressed current IIOs targeting Sweden, for example in response to attempts by malicious actors to undermine Sweden´s accession process to NATO.

Conclusion

In conclusion, Sweden's approach to countering IIOs is based on a dedicated agency for psychological defence and the overarching system of total defence, involving whole-of-society efforts and close cooperation between several government agencies. Recent events, such as the LVU campaign and Quran burnings, and the 2024 Eurovision Song Contest in Malmö, have tested Sweden's capabilities and provided important lessons for the future.

Key takeaways

- Sweden prioritises resilience-building efforts involving all of society within the frame of total defence, with the purpose of creating a solid foundation to counter IIOs.
- Unlike the other Nordic-Baltic countries, Sweden has a governmental agency specifically dedicated to psychological defence.
- Communication campaigns and leaflets are devised to address the population directly, to make citizens aware that they are an integral part of the total defence system.

Discussion

The NB8 countries use a mix of strategic approaches including specific state strategies towards IIOs, coupled with broader national security strategies. Pre-emptive measures seem to be the most common taken, with resilience-building efforts being a focal point for all countries. Reactive responses are often conducted by civil society or media outlets fact-checking specific narratives, although state actors might sometimes address the issue depending on the scale. This could take the shape of, for example, press conferences or the public release of declassified documents. Media regulators sometimes also limit the broadcasting of a certain outlet.

There are many takeaways for other countries faced with the same or similar threats. Key ones include having a whole-of-society approach to both the pre-emptive and reactive ways to counter IIOs, involving both civil society and the media as much as possible. Here we can note several important examples, including involving civil society organisations in exercises and education, as well as supporting fact-checking organisations financially and through other means.

Furthermore, close public cooperation is of the essence, given that the threat usually targets multiple sectors in society. Here we can note different models within the region, although a commonality for many is flexible coordination structures allowing for rapid and responsive reactions. The public is also a key actor and there are many good examples of NB8 countries, through communications and other projects, bolstering citizen resilience. This includes informing citizens about information-based threats, potential targeting methods employed by threat actors, and practical self-protection measures, while ensuring transparency about the current threat environment. Much of the core knowledge for these initiatives can be shared.

Aside from the many best practices, NB8 countries also face dilemmas in developing strategies and implementing measures. We outline some of these below:

- **Balancing freedom of speech while introducing disruptive countermeasures:** Resilience measures can only take you so far. In order to deter and limit the spread of IIOs, disruptive measures might be necessary. Here it varies across the region to what extent states can implement such measures, given the different national legislations. An important balance to strike is to be able to disrupt certain actions by hostile actors, but at the same time not grant too extensive powers to governments.

- **Informing the media**: The media play an important role as the providers of factual information to the public. It is a difficult task given the vast amount of false and misleading information circulating in the information environment. Thus, states might assist the media in this effort by providing information about current incidents and guidance on identified operations. This needs to be done in a balanced way to avoid being prescriptive.

- **Involvement of civil society:** An important aspect of countering IIOs is the involvement of civil society. Here governments need to balance the efficiency of outsourcing with security aspects. A key factor is also how to ensure that the civil society actors engaged in countering activities are protected and take the right safety precautions.

- **When to respond:** Choosing when to highlight an identified campaign and possibly respond is a key challenge. On the one hand, highlighting an incident can be beneficial for raising threat awareness domestically and signalling state awareness of the problem – on the other hand, highlighting

an influence activity might also give the threat actor the visibility it seeks.

- **Engagement in international forums:** Although it is generally positive that there are several forums where countries can share best practices and exchange valuable information, the vast number puts strains on resources, and countries have difficult choices over which to prioritise.

Finally, we believe that the NB8 forum has a lot of potential for joint cooperation in this field, given the relatively similar approaches of countries tackling the issues and the relatively similar threat (although scale and urgency differ). This was also confirmed via several interviews where participants highlighted an appetite for deepened regional cooperation. However, this would require taking existing international cooperation structures such as the NATO RRG and EU RAS into account, in order not to duplicate effort but to complement it.

Below we outline some suggestions about deeper regional cooperation:

1. Consider establishing a **shared comprehensive capability development framework,** encompassing structured checklists and training modules for all stakeholders involved in countering IIOs. The framework could be supported by the International Organization for Standardization (ISO), the US National Institute of Standards and Technology (NIST), or EU certification. This includes setting clear objectives, capability goals, and pathways for non-state actors to develop or enhance their own competencies.

2. Consider designating **capability leaders** among NB8 countries, where one country takes the lead in sharing its expertise on specific aspects of IIO defence (e.g., threat intelligence or media literacy programmes). This would foster knowledge transfer within the NB8 and ensure a holistic development approach to countering threats more effectively based on relative strengths.

3. Regularly **conduct shared exercises** simulating diverse scenarios that test the collective readiness and response capabilities across the NB8 nations. These drills should emphasise joint threat assessments and encourage a coordinated approach to leveraging each nation's unique strengths in areas such as strategic communication or deterrence work.

4. Consider developing and testing a **common proactive response project** to assess cooperation, strategy, and tradecraft. The goal should be more than 'coordinated tweets from the capitals' and should demonstrate the value of coordinated offensive responses to penetrate hostile information environments, in preparation for a sudden escalation from threat actors. This would need to be prepared for in close cooperation with NATO and its plans and procedures.

Conclusion

This study shows that, in many ways, countries in the NB8 region might be considered leaders in countering IIOs. Often this is down to a strong sense of shared responsibility for society: shared between government departments and agencies, combined with the very active participation of civil society.

The report has focused on outlining the most visible approaches, capabilities, and measures among the NB8 countries and the region as a whole. Future research could potentially go deeper, through a capability assessment that uses grading methods to compare process maturity, for example. Such an approach would be needed to accurately compare different capabilities' effectiveness and efficiencies, but to do so all NB8 countries would need to agree to share more granular information about their work, and the results would most likely not be publicly available.

It could also be beneficial to evaluate examples of implemented countermeasures more thoroughly through assessments or studies of effect, perhaps leading towards comprehensive reporting of significant initiatives and their outcomes across the region. This would include security policy and deterrence activities, in addition to strategic communication and resilience-building initiatives. Such a study could strongly complement capability development efforts and help to share best practices among NB8 partners. Such a report would, however, most likely be shared within government circles only.

Finally, given that the countries in the region face a similar threat from known actors, more joint initiatives including training, education, and pre-emptive responses would enhance the overall capability in the region. It is our hope that this report could be a point of departure for more initiatives benefiting all.

Bibliography

Main report

Ahonen, A., Bilal, A., Hoogensen Gjørv, Jurāns, J., Kragh, M., Krūmiņš, K.K., Lange-Ionatamishvili, E., Liubinavičius, B., Mikulski, K., Mölder, H., Ólafsson, J.G., Ómarsdóttir, S.B., Sazonov, V. and Serritzlev, J. ***Russia's Information Influence Operations in the Nordic-Baltic Region***. NATO Strategic Communications Centre of Excellence, November 2024.

Andrijauskas, K. ***'Chinese influence in Lithuania'***. CEPA, 2 August 2022.

Pamment, J. ***A Capability Definition and Assessment Framework for Countering Disinformation, Information Influence and Foreign Interference.*** NATO Strategic Communications Centre of Excellence: 2022.

Sundqvist, G. and Lindberg, F. ***´Statliga kinesiska påverkansopeationer mot demokratin i Svenska kommuner´***. Myndigheten för psykologiskt försvar, 2022.

Country profiles

Denmark

Interview

Interview with representatives from the Ministry of Foreign Affairs of Denmark, May 2025

Policy documents and legislation

Folketinget. ***'Evaluering af den tværministerielle task force til imødegåelse af påvirkningsoperationer'*** [Evaluation of the inter-ministerial task force to address the impact of operations], 2020.

Forsvarets Efterretningstjeneste & Politiets Efterretningstjeneste. '***Vurdering af truslen for påvirkningsvirksomhed fra fremmede stater i forbindelse med valget til Inatsisartut i 2025'*** [Assessment of the threat of influence activities from foreign states in connection with the 2025 Inatsisartut elections], 2025.

Ministry of Foreign Affairs of Denmark. ***The Ministry of Foreign Affairs of Denmark's Strategy for Tech Diplomacy***, May 2024.

Politiets Efterretningstjeneste. ***'Threats to Denmark'***.

Styrelsen for Samfundssikkerhed. ***Nationalt Risikobillede*** [National risk picture]. Styrelsen for Samfundssikkerhed, 2025.

Other sources

Justitsministeriet. *'Styrket værn mod udenlandsk påvirkning af danske valg og demokratiet'* [Strengthened protection against foreign influence on Danish elections and democracy]', 7 September 2018.

Ministry of Defence. *'Strengthened safeguards against foreign influence on Danish elections and democracy'*, 7 September 2018.

Ministry of Foreign Affairs of Denmark. *'Office of Denmark's Tech Ambassador'*.

Politiets Efterretningstjeneste. *'Ingen systematisk og koordineret påvirkning af det danske valg til Europa-Parlamentet'* [No systematic and coordinated influence on the Danish elections to the European Parliament], 24 June 2024.

Politiets Efterretningstjeneste. *'Ingen tegn på påvirkning af valget til Inatsisartut fra fremmede efterretningstjenester'* [No signs of influence on the Inatsisartut election by foreign intelligence services], 2025.

Politiets Efterretningstjeneste. *'Myndighederne holder øje med mulig påvirkning fra fremmede stater i forbindelse med valget til Inatsisartut'* [Authorities are monitoring possible influence from foreign states in connection with the Inatsisartut elections], 2025.

Politiets Efterretningstjeneste. *'Påvirkningsvirksomhed fra fremmede stater'* [Influence activities from foreign states], 2025.

Politiets Efterretningstjeneste. *'PET og FE holder øje med mulig påvirkning fra fremmede stater af dansk EU-valg'* [PET and FE are monitoring possible influence from foreign states on Danish EU elections], 30 May 2024.

Estonia

Interviews

Interview with representatives from the Estonian Defence Forces, 4 February 2025

Interview with representatives from the Estonian Internal Security Service (KAPO), 5 February 2025

Interview with representatives from the Government Office Strategic Communications Department, 4 February 2025

Interview with representatives from the Ministry of Defence, 5 February 2025

Interview with strategic communications expert Mr Raul Rebane, 4 February 2025

Policy documents and legislation

Government of the Republic of Estonia. *National Security Concept of Estonia*, 2023.

Ministry of Education and Research of the Republic of Estonia. *'Transition to Estonian-language education'*, 2024.

Parliament of Estonia. *'Eesti Vabariigi põhiseaduse muutmise seadus 536 SE'* [Act on Amendments to the Constitution of the Republic of Estonia 536 SE], 2025.

Parliament of Estonia. *'Kirikute ja koguduste seaduse muutmise seadus 570 SE II'* [Churches and Congregation Act Amendment Act 570 SE II], 9 April 2025.

State Chancellery of the Republic of Estonia. *Riigikaitse arengukava 2022–2031* [National Defence Development Plan, 2022–2031], 2022.

Academic references

Hardy, E. *'Estonian broadcast bill targets Russian propaganda, but raises questions over online content'*, *Parliament Magazine*, 28 April 2025.

Juurvee, I. and Mattiisen, A.M. *'The Bronze Soldier Crisis of 2007: Revisiting an Early Case of Hybrid Conflict'*, International Centre for Defence and Security, August 2020.

Mölder, H. and Sazonov, V. 'Estonia.' In Ahonen, A., Bilal, A., Hoogensen Gjørv, Jurāns, J. Kragh, M., Krūmiņš, K.K., Lange-Ionatamishvili, E., Liubinavičius, B., Mikulski, K., Mölder, H., Ólafsson, J.G., Ómarsdóttir, S.B., Sazonov, V. & Serritzlev, J. '*Russia's Information Influence Operations in the Nordic-Baltic Region'*. NATO Strategic Communications Centre of Excellence, November 2024.

Ostamaa, M. *'Amendments to authorize Estonian regulator to restrict propaganda broadcasts'*, *EER*, 21 April 2025.

Other sources

EER. *'Survey: Kremlin channels lose significance with Russian-speakers in Estonia'*, 12 April 2020.

Estonian Internal Security Service. *Annual Review*, 2024–2025, 2025.

Government of the Republic of Estonia. *'Government introduces a sanction to defend against hostile influence activities by Russia and Belarus'*, 2024.

Open Society Institute. *'Finland tops the new Media Literacy Index'*, 24 June 2023.

Parliament of Estonia. *'The Riigikogu banned using of symbols supporting acts of aggression by foreign states'*, 21 April 2022.

Palloson, M. *'Russia's intelligence interest in Estonia remains consistent. Opinion'*, 14 April 2025.

Propastop.

Reporters Without Borders. *'World Press Freedom Index'*, 2025.

Finland

Interviews

Interview with Dr Päivi Tampere, former head of the Strategic Communications Department, Office of the Prime Minister, 8 April 2025

Interview with representatives from the Finnish Defence Forces, 10 April 2025

Interview with representatives from the Finnish Security Intelligence Service (SUPO), 9 April 2025

Interview with representatives from the Finnish Transport and Communications Authority (TRAFICOM), 9 April 2025

Interview with representatives from the Ministry of Foreign Affairs, 10 April 2025

Written comments submitted by representatives from the Ministry of Defence

Policy documents and legislation

Sisäministeriö. *'National risk assessment'*, 2023.

Turvallisuukoomitea. '*Security Strategy for Society'*, 2025.

Other sources

Finnish Government. *'Overview of information influence activities'*, 2025.

Mediapooli.

National Cyber Security Centre Finland. *'Weekly review of NCSC-FI'*.

National Defence Training Association of Finland. *'Informaatiovaikuttaminen'* [Information influence], 2025.

Reuters. *'Fact check: Video shows Finland moving tanks to planned military exercise, not to Russian border'*, 5 May 2025.

University of Jyväskylä. *'Kansalaisen informaatioturvallisuus'* [Citizen information security].

Iceland

Interviews

Interview with Icelandic academics specialising in strategic communications, 29 April 2025

Interview with representatives from the Icelandic Media Commission, 28 April 2025

Interview with representatives from the Icelandic Ministry for Foreign Affairs, 28 April 2025

Interview with representatives from the Liaison Group of the National Security Council, 29 April 2025

Interview with representatives from the Office of National Commissioner of the Icelandic Police, 29 April 2025

Policy documents and legislation

Althingi. *'Lög um bann við fjárhagslegum stuðningi erlendra aðila við íslenska stjórnmálaflokka og blaðaútgáfu erlendra sendiráða á Íslandi'* [Act on the prohibition of financial support by foreign parties to Icelandic political parties and the press publications of foreign embassies in Iceland], 2020.

Government of Iceland. *'National security'*, 2023.

Icelandic Media Commission. *Upplýsingaóreiða og skautun í íslensku samfélagi* [Information chaos and polarisation in Icelandic society], 2023.

National Commissioner of the Icelandic Police. *'Fjölþáttaógnir'* [Multifaceted threats], 8 March 2023.

Parliamentary Resolution on a national security policy for Iceland, No. 26/145, 13 April 2016, amended on 28 February 2023.

Other sources

Government of Iceland National Security Council. *Hybrid Threats: Summary Report. National Security Council conference on hybrid threats held at the University of Iceland*, February 2020.

Icelandic Media Commission. *'Svona þekkir þú rangfærslur og falsfréttir'* [How to recognise misinformation and fake news], 2023.

National Security Council. *Report of the National Security Council's Working Group on Information Disorder and COVID-19*, October 2020.

Organisation for Economic Co-operation and Development. *'OECD survey on drivers of trust in public institutions 2024 results – country notes: Iceland'*, 10 July 2024.

Latvia

Interviews

Interview with representatives from the Ministry of Defence and Latvian Armed Forces, 19 February 2025

Interview with representatives from the Ministry of Foreign Affairs, 17 February 2025

Interview with representatives from the National Electronic Media Council, 25 March 2025

Interview with representatives from the State Security Service, March 2025

Interview with representatives from the Strategic Communications Department of the State Chancellery, 19 February 2025

Policy documents

Cabinet of Ministers of the Republic of Latvia. *'The national concept on strategic communication and security of the information space (2023–2027)'*, 20 March 2023.

Latvian Ministry of Defence. *The State Defence Concept*, 2023.

Other sources

LSM. *'Lūdz sākt kriminālvajāšanu pret 6 organizācijas "Baltijas Antifašisti" izveidotājiem'* [Requests to initiate criminal prosecution against 6 founders of the organisation 'Baltic Antifascists'], 13 October 2023.

LV portals. *'VDD: Latvijas sabiedrība saglabā noturību pret Krievijas kara propaganda'* [VDD: Latvian society remains resilient against Russian war propaganda], 12 March 2024.

Nacionālā elektronisko plašsaziņas līdzekļu padome. *'Medijpratības datubāze'* [Media literacy database], 2025.

Nacionālā elektronisko plašsaziņas līdzekļu padome. *'Piekļuves ierobežošana tīmekļa vietnēm'* [Guidelines and statistics on restricting the access to websites], 2022.

State Chancellery. *Handbook Against Disinformation: Recognise and Resist*. Riga, October 2025.

Teperik, D., Bankauskaite, D. and Struberga, S. *'Examining societal resilience in the Baltics – a public outlook.'* Latvian Transatlantic Organisation, 2024.

TV3 Ziņas. *'Bijušais Rīgas domnieks Pankratovs aizbēdzis uz Krieviju un brāļojas ar propagandistiem'* [Former Riga councillor Pankratov has fled to Russia and is fraternising with propagandists], 13 November 2023.

Lithuania

Interviews

Interview with representatives from the Civil Resistance Initiative (CRI), 12 February 2025

Interview with representatives from the Department of Civil Resistance, Ministry of Defence, 11 February 2025

Interview with representatives from the Ministry of Defence, 12 February 2025

Interview with representatives from the Ministry of Foreign Affairs of Lithuania, 12 February 2025

Interview with representatives from the Lithuanian Radio and Television Commission, 25 March 2025

Interview with representatives from the Lithuanian Riflemen's Union, 13 February 2025

Interview with representatives from the National Crisis Management Centre, 12 February 2025

Interview with representatives from the Strategic Communications Department of the Armed Forces of Lithuania, 12 February 2025

Policy and legislative documents

Defence Intelligence and Security Service under the Ministry of National Defence and State Security Department of the Republic of Lithuania. *National Threat Assessment*, 2022.

Government of the Republic of Lithuania. *National Security Strategy of the Republic of Lithuania*, 2021.

Seimas of the Republic of Lithuania. *'Lietuvos Respublikos visuomenės informavimo įstatymas'* [Republic of Lithuania public information law], 1 July 2025.

Seimas of the Republic of Lithuania. *'Resolution Amending Resolution No IX-907 of the Seimas of the Republic of Lithuania of 28 May 2002 on the Approval of the National Security Strategy'*, 16 December 2021.

Other sources

Andrijauskas, K. *'Chinese Influence in Lithuania'*. CEPA, 2 August 2022.

Debunk.org. *'About elves'*.

Council of the European Union. *'EU imposes sanctions on state-owned outlets RT/Russia Today and Sputnik's broadcasting in the EU'*, 2 March 2022.

DISARM Foundation. *'DISARM Red Framework'*.

Lithuanian Radio and Television Commission. *'Asmenų, neteisėtai vykdančių televizijos programų ir (ar) atskirų programų platinimo internete Lietuvos Respublikos vartotojams veiklą, sąrašas'* [List of persons who provide illegal services of distribution of television programmes and/or individual programmes for users of the Republic of Lithuania online].

Lithuanian Radio and Television Commission. *'Ribojimai, susiję su tarptautinių sankcijų įgyvendinimu'* [Restricted IP and domain services due to implemented EU sanctions].

Ministry of National Defence of the Republic of Lithuania. *'Minister of National Defence L. Kasčiūnas signs an agreement as Lithuania comes a step closer to the stationing of a German brigade'*, 13 September 2024.

Norway

Interviews

Interview with representatives from the Armed Forces, 23 April 2025

Interview with representatives from the Ministry of Culture, 23 April 2025

Interview with representatives from the Ministry of Defence, 23 April 2025

Interview with representatives from the Ministry of Foreign Affairs, 23 April 2025

Interview with representatives from the Ministry of Justice, 23 April 2025

Interview with representatives from the National Security Agency, 23 April 2025

Interview with researcher Eskil Sivertsen, Norwegian Defence Research Establishment (FFI)

Policy and legislative documents

Council of Europe. *'RESIST – Strengthening Societal Resilience to Disinformation in Europe'*, 18 September 2025.

Government of Norway. *'Lov om nasjonal sikkerhet (sikkerhetsloven)'* [National Security Act (Security Act)], 2019.

Ministry of Justice. *'Total preparedness, Meld. St. 9 (2024–2025) report to the Storting (white paper)'*, 2025.

Office of the Prime Minister of Norway. *'National security strategy'*, 8 May 2025.

Regjeringen. *'Keeping the children safe: A shared responsibility'*, 14 April 2016.

Regjeringen. *'NOU 2023: 17: Nå er det alvor. Rustet for en usikker fremtid'* [NOU 2023: 17: Now it's serious. Prepared for an uncertain future)], 2023.

Regjeringen. *'Strategi for å styrjke motstandskrafta mot desinformasjon (2025–2030)'* [Strategy to strengthen resilience against disinformation (2025–2030)], 16 June 2025.

Stortinget. *'Vedtak til lov om endringer i politiloven og politiregisterloven (PSTs etterretningsoppdrag og bruk av åpent tilgjengelig informasjon)'* [Resolution on amendments to the Police Act and the Police Register Act (PST's intelligence mission and use of openly available information)], 2023.

Stortinget. *'Vedtak til lov om endringer i straffeloven mv. (påvirkning fra fremmed etterretning)'* Resolution on the Act on Amendments to the Criminal Code, etc. (influence from foreign intelligence)], 2024.

Other

EUvsDisinfo. *'Disinfo: Child protection service took at least one child from more than half of Norwegian families'*, 5 August 2020.

Faktisk. *'Et samarbeid om påvirkning'* [A collaboration for influence].

Faktisk. *'Faktasjekkere utsatt for prorussisk kampanje'* [Fact checkers exposed to pro-Russian campaign], 4 June 2024.

Sweden

Interviews

Interview with representatives from the Ministry of Culture, 28 March 2025

Interview with representatives from the Ministry of Defence, 26 March 2025

Interview with representatives from the Ministry of Foreign Affairs, 27 March 2025

Interview with representatives from the Ministry of Justice, 27 March 2025

Interview with representatives from the Prime Minister's Office, 27 March 2025

Interview with representatives from the Psychological Defence Agency, 26 March 2025

Written comments received from the Swedish Armed Forces

Policy and legislative documents

Government Offices of Sweden. *'National security strategy'*, 8 July 2024.

Other sources

Psychological Defence Agency. *Don't Be Fooled: A Handbook to Help You Recognise and Deal with Disinformation, Misleading Information and Propaganda,* 2023.

Psychological Defence Agency. *'Förmågeportalen'* [The ability portal], 2025.

Psychological Defence Agency. *'Our mission'*, 2025.

Psychological Defence Agency. *'Statliga kinesiska påverkansoperationer mot demokratin i svenska kommuner'* [Chinese state influence operations against democracy in Swedish municipalities], 2022.

Regeringen. *'Pressträff om åtgärder mot LVU-kampanjen'* [Press conference on measures against the LVU campaign], 2 February 2023.

Sveriges Television. *'Ministern: Ryskstödda aktörer vill skada Sverige'* [Minister: Russian-backed actors want to harm Sweden], 12 December 2023.

Sveriges Television. *'Så bidrog LVU-kampanjen till höjd terrorhotnivå: "Anklagelser om systematisk barnhandel"'* [How the LVU campaign contributed to a heightened terrorist threat level: 'Allegations of systematic child trafficking'], 11 November 2024.

Swedish Civil Contingencies Agency. *'Download or order the brochure In case of crisis or war'*, 2024.

Prepared and published by the
NATO STRATEGIC COMMUNICATIONS
CENTRE OF EXCELLENCE

The NATO Strategic Communications Centre of Excellence (NATO StratCom COE) is a NATO accredited multi-national organisation that conducts research, publishes studies, and provides strategic communications training for government and military personnel. Our mission is to make a positive contribution to Alliance's understanding of strategic communications and to facilitate accurate, appropriate, and timely communication among its members as objectives and roles emerge and evolve in the rapidly changing information environment.

www.stratcomcoe.org | @stratcomcoe | info@stratcomcoe.org