COMMUNICATING THE RUSSIAN THREAT: INTELLIGENCE AGENCIES' PUBLIC MESSAGING IN EUROPE (2025)

DOI: https://doi.org/10.37458/nstf.26.2.6
Review paper
Received: October 2, 2025
Accepted: November 12, 2025

Lotte Nietzman[*], **Peter Schrijver**[**]

Abstract: Recent Statements by NATO Secretary General Mark Rutte and former Lithuanian Foreign Minister Gabrielius Landsbergis have emphasised the security concerns as a result of the threats posed by Russia (NATO, 2025a; Ukrainian World Congress, 2025). While European intelligence agencies traditionally

[*] Lotte Nietzman MSc is researcher Cyber Operations at the War Studies Research Centre of the Netherlands Defence Academy (NLDA). She can be reached at l.nietzman.01@mindef.nl. For further information see https://orcid.org/0009-0004-4939-1409.

[**] Peter Schrijver is PhD Candidate at the NLDA and researcher at Leiden University. He can be reached at p.schrijver@mindef.nl. For further information see https://orcid.org/0009-0004-6526-0150.

operate within limited public visibility, they increasingly communicate about Russian threats through public reports – not merely for transparency, but as part of their institutional role in democratic societies.

As the primary entities responsible for monitoring such threats, intelligence agencies play a crucial role in shaping public understanding. This research examines how European intelligence agencies communicate about the Russian threat through their 2025 annual reports and threat assessments. By analysing publications from Denmark, Estonia, Norway, Finland, Latvia, Sweden and the Netherlands, the study investigates the communication strategies used to inform and influence public perceptions of Russian activities.

Employing intelligence communication theory as its primary analytical lens, the study explores how intelligence agencies convey complex threat information to their audiences while balancing transparency and operational security (Petersen, 2019). By focusing on a specific year and a selected set of European countries, the study provides a comparative snapshot of intelligence communication practices in response to Russian security threats.

The research applies thematic analysis to identify key themes, narratives, patterns and frames used within the reports (Braun, & Clarke, 2022). This method allows for a systematic examination of how intelligence agencies articulate threats, structure their messages, and frame Russian activities for public consumption. The findings contribute to a better understanding of the role of intelligence agencies in public discourse, offering insights into the intersection of intelligence, media and strategic communication (Schrijver, Nietzman, & Pijpers, 2025).

This research will be of interest to scholars of intelligence studies, security studies, and political communication, as well as practitioners seeking to refine intelligence messaging strategies. The findings also hold relevance for policymakers on how to communicate security threats in democratic societies.

Keywords: Strategic Communication, Intelligence, Transparency, Operational Security.

Introduction

Intelligence agencies have come a long way when it comes to communicating to the public. This is explained by the fact that historically, intelligence agencies have prioritised the protection of sources and methods above anything else, operating with minimal public visibility. Since the end of the Cold War, however, liberal international relations theorists argued that secrecy can undermine international cooperation and increase the risk of conflict (Pew Research Centre, 2015). From the realist perspective security remains vital for national survival and strategic advantage. While liberal theorists advocate for transparency to foster cooperation, realist scholars caution that excessive openness may compromise this strategic advantage (Williams, & McDonald, 2023, p. 43; Doyle, 1983, p. 323). This tension underscores the delicate balance intelligence agencies must strike.

Alongside these debates, technological advances over the last fifteen years have created new ways to share information, prompting intelligence agencies to become more visible. They increasingly recognised not only the necessity of greater transparency and accountability for

sustaining public trust, but also the strategic potential of communication in democratic societies (Zegart, & Morrell, 2019). The revelation of the U.S. National Security Agency's mass surveillance techniques by Edward Snowden in 2013 led to another push for greater transparency. (McLoughlin, Ward, Lomas, 2020, p. 233).

These shifts coincide with the wider adoption of a whole-of-society approach to security, especially across Europe (Jermalavičius, & Parmak, 2014, p. 24). This framework envisions resilience as a shared mission: national defence is not only the responsibility of state institutions, but also of civil society, private sector actors, and the broader public (Wigell, Mikkola, & Juntunen, 2021, p. 19). In policy circles, this concept has been applied in contexts such as hybrid-threat response, total defence and disinformation resilience (Zdanavičius, & Statkus, 2020, p. 1). Consequently, public communication by intelligence agencies has acquired new significance, not merely as transparency, but as tool to raise public awareness and strengthen social resilience.

Yet it remains unclear how far this whole-of-society ambition is reflected in practice. While intelligence organisations in Western democracies have intensified their communication strategies, the extent to which their annual threat assessments and public reports embody the principles of broad societal engagement has not been systematically examined.

Since the start of the 21st century, intelligence organisations underwent a transformation from covert to overt action. Intelligence agencies around the world are

becoming much more visible as they realise, they could actually use new media to their advantage and simultaneously understand that they need to be more transparent and open to scrutiny if they are to maintain public support (Magen, 2017, p. 272). The result is a great diversity of communication practices by Western intelligence organisations (Petersen, 2019, p. 317). Several examples of overt communication practices include public (annual) threat assessments, parliamentary testimonies by intelligence leaders, social media engagement by agencies like MI5, CIA and NSA that now actively maintain their own social media accounts, agencies declassifying reports and historical archives. This article examines the above-mentioned question by analysing how European intelligence agencies communicate about the Russian threat through their 2025 annual reports.

By analysing publications from Denmark, Estonia, Finland, Latvia, Norway, Sweden and the Netherlands, the study investigates whether these reports function primarily as traditional intelligence updates or whether they also serve as instruments of the whole-of-society approach, designed to inform and influence public perceptions of Russian activities. The study employs thematic analysis to uncover recurring themes, narrative structures and framing patterns within the reports. This approach systemically investigates how intelligence agencies construct threat discourses, organise their communication and present Russian activities to shape public understanding.

The Russian threat should however not be seen as a regional concern but as part of a global narrative. Waging a hybrid war against multiple countries in which

disinformation campaigns, sabotage activities and cyber threats are the rule rather than the exception, Russia is shaping public and institutional responses all around the world.

Literature Review

This section examines the literature on mediatisation and intelligence communication, outlining how the pressure of contemporary media environments creates tensions and opportunities for intelligence organisations and explaining why these traditionally secretive institutions have developed public communication strategies in the first place. It also functions as setup for this study's theoretical framework.

Mediatisation

Mediatisation refers to the process in which media have become increasingly influential in and deeply integrated into different spheres of society (Strömbäck, & Esser, 2014, p. 376). It describes how governmental and societal institutions adapt to media logic by reshaping their practices to meet expectations for immediacy, participation, and transparency. These characteristics are particularly relevant to intelligence agencies, where the traditionally secretive nature of operations increasingly intersects with demands for openness.

The manifestation of mediatisation can be understood through three characteristics that shape institutional adaptation to media logic**.** First, immediacy refers to the rapid exchange of information enabled by modern media technologies. The speed of communication reduces delays, creating expectations for swift responses and continuous engagement. This dynamic pushes

institutions to operate in ways that keep pace with fast-moving media cycles (Zeitzoff, 2017, p. 1378). However, such rapid communication can lead to challenges, including the risk of spreading disinformation, difficulty in verifying facts, and reduced opportunities for deliberate decision-making (Zeitzoff, 2017, p. 1378).

Second, mediatisation also entails participation by enabling wider public engagement in processes traditionally controlled by institutions. Social media and digital platforms facilitate a more interactive and inclusive flow of information, allowing audiences to contribute content and engage in dialogue (Yanchenko, 2021, p. 277).

Transparency, a third dimension of mediatisation, reflects growing demands for openness in how institutions operate and communicate. Media technologies amplify public expectations for accountability, requiring institutions to disclose information more frequently and justify their actions (Magen, 2017, p. 269). Balancing this demand with the need for confidentiality requires careful navigation (Hulnick, 1999, p. 481). Mediatisation is a reciprocal process: the media influences institutional behaviour, while institutions seek to shape media platforms to serve their own interests (Krotz, 2017, p. 103).

This societal influence has led to a growing role of public-facing communication in intelligence work, defined by Petersen as intelligence communication: 'The strategic use of information by intelligence agencies to engage with and influence the public' (Petersen, 2019, p. 317). Historically, this meant balancing secrecy with

controlled disclosure and prioritizing discretion over public engagement (Gill, & Phythian, 2018, p. 469). Yet, as Magen observes, this tradition increasingly meets rising expectations for transparency (Magen, 2017, p. 269). One response has been the expansion of external communication by intelligence organisations, which now extends beyond traditional press statements to include active use of websites and social media platforms for both broadcasting information and soliciting public participation (Petersen, 2019, p. 317).

These trends are intensified by broader changes in the information environment. The growth of social media over the past two decades, combined with transparency demands by public interest groups, has further reshaped how intelligence agencies manage their public messaging (Aldrich, & Moran, 2018, p. 25). Their ability to control information has diminished, as open-source research collectives and other independent actors increasingly publish findings that challenge official narratives (Puyvelde, 2013, p. 139). For organisations accustomed to secrecy, such developments intensify the need to adapt.

Intelligence communication and the performance gap

This inherent tension between secrecy and visibility is part of a wider institutional challenge for intelligence organisations that Petersen terms the 'performance gap': the struggle to meet high public and political expectations of effectiveness despite inherent operational limitations (Petersen, 2019, p. 318). In this context, intelligence communication has become a strategic tool for managing this gap, reinforcing institutional legitimacy and demonstrating relevance in

an era of expanding oversight, evaluation, and public scrutiny. This shift has moved intelligence agencies from the periphery of public discourse to active participants within a competitive, mediatised environment (Schrijver, Nietzman, & Pijpers, 2025).

To manage these pressures and use the media environment strategically, intelligence agencies disclose information selectively, aligning releases with strategic objectives while protecting sources and methods (Riemer and Sobelman, 2023, p. 5). This tactical transparency involves controlled, purposeful disclosures that aims to bolster credibility, counter adversary messaging, and signal operational effectiveness.

A related practice is 'coercive intelligence disclosure', the deliberate release of intelligence to influence adversary decision-making (Riemer, & Sobelman, 2023, p. 2). These disclosures aim to achieve 'narrative superiority', with the timing and content of releases carefully managed to support a preferred framing of events (Dylan, & Maguire, 2022). Closely related is the term 'warning intelligence'. According to Cynthia M. Grabo, this should be seen as intelligence that is specifically intended to be predictive, focusing on identifying potential threats before they materialise (Akrap, Mandić, & Žigo, 2022, p. 1264). Disclosures of this kind may also reassure allies, or signal foresight and credibility to domestic audiences. While the underlying sources may remain classified, the publication of intelligence-related material functions as a tool of influence (Dylan, & Maguire 2022, p. 47). The mediatised environment amplifies these effects, as disclosed intelligence circulates rapidly online and informs public opinion.

Despite these moves toward a calculated form of openness, such communications remain constrained. They are typically centrally directed and occasional, rather than forming a sustained dialogue with the public (Petersen, 2019, p. 320) (Avidar, & Magen, 2023, p. 6). Although agencies have begun testing more consistent forms of engagement, the dominant model still prioritises control and restricts interaction with external audiences (McLoughlin, Ward, & Lomas, 2020, p. 233) (Landon-Murray, 2015, p. 67).

Nevertheless, in partnership with private cyber security organisations, some western intelligence agencies have taken a more collaborative approach in which they treat private companies as equal in order to create and communicate mutual understanding of the cyber threat (Petersen, 2019, p. 321). In the context of the Russo-Ukrainian war, Ukraine's military intelligence directorate (HUR) has taken this collaborative approach even further. Its sustained use of messaging platform Telegram combines domestic audience engagement, psychological pressure on the adversary, and public contributions to intelligence work (Schrijver, 2025, p. 20). Civilians are incorporated not only as recipients of information, but as active participants in intelligence collection, tactical support, and strategic messaging, an approach that goes beyond the parameters of most peacetime intelligence communication (Schrijver, 2025, p. 20).

In Petersen's framework, three distinct forms of intelligence communication with the public, each characterised by various levels of openness and cooperation with outside actors, are identified (Petersen, 2019, p. 317). This research takes her framework as its

starting point to examine how European intelligence organisations communicate the Russian threat in an increasingly mediatised environment.

Theoretical Framework: Concepts of Intelligence Communication

In her article, "Three concepts of intelligence communication: Awareness, advice or co-production?" Karen Lund Petersen (2019) distinguishes between three approaches intelligence agencies use when communicating to the public.

The first approach, 'Awareness', focuses on informing the public about potential threats or risks and is often carried out through public announcements or media campaigns. This approach is not aimed at provoking action but rather serves to create democratic accountability by promoting general public awareness. It revolves around the tension between openness and secrecy, as secrecy is deemed essential for national security purposes and openness is needed for democratic debate (Petersen, 2019, p. 319). Communication in this regard is seen as a means to enable the public to understand or trust the actions of the authorities.

'Advice' goes one step further than simply informing the public and rather aims to provide specific guidance or recommendations on how to respond to a threat. In this approach the public is viewed as an active player who can respond to requests from the intelligence service (Petersen, 2019, p. 320). The goal is to stimulate effectiveness and action by disseminating knowledge. Intelligence information in this regard is presented as expert knowledge that objectively maps threats and risks and is passed on to the public in order to enable them to

make informed decisions. Today this has primarily been used in the context of counterterrorism: Intelligence organisations advising governments or citizens on taking on or refraining from actions, based on a terrorist threat. An example of this is the implementation of additional security in conjunction with increasing threat levels.

Third, 'Co-production' recognises the public as active participants in the intelligence process, insofar that intelligence agencies might ask citizens to work in partnerships with them in identifying and addressing threats. This third concept reflects a shift from the traditional 'government to governance' approach as it recognizes the fact that security management takes place outside traditional state bureaucracies, often in fragmented public and private spheres (Petersen, 2019, p. 320). From this perspective, 'Awareness' and 'Advice' are based on a hierarchical relationship: Intelligence organisations possess certain knowledge that they may or may not share with the public. 'Co-production' in this sense is more egalitarian. Intelligence organisations understand they do not necessarily have a monopoly on wisdom and may want to appeal to citizens or other actors in society.

The focus is on mobilising and involving various societal groups to share information and/or to be better prepared for possible future threats. The three concepts represent different ways in which intelligence agencies engage with the public – each with its own implications for public trust and the effectiveness of security measures.

Methodology

Employing intelligence communication theory as its primary analytical lens, the study explores how

intelligence agencies convey complex threat information to their audiences while balancing transparency and operational security. By focusing on a specific year and a selected set of Northern and Western European countries, the study provides a comparative snapshot of intelligence communication practices in response to Russian security threats. The study includes the Nordic Countries as well as two Baltic states, given their proximity to the Russian Federation. The sample also encompasses The Netherlands in order to include the Western European gaze in the study as well.

The research applies thematic analysis to identify key themes, narratives, patterns, and frames used within the reports. This method allows for a systematic examination of how intelligence agencies articulate threats, structure their messages, and frame Russian activities for public consumption. The findings contribute to a better understanding of the role of intelligence agencies in public discourse, offering insights into the intersection of intelligence, media, and strategic communication.

Ten initial themes were formulated:

- hybrid warfare and information warfare
- sabotage activities
- cyber operations
- espionage and undercover operations
- nuclear threats
- military build-up and an uncertain future
- Russian military build-up
- public awareness and preventive counselling
- military partnerships, and
- military technology.

These themes were used as starting point for coding. While reading the annual report systemically, themes were revised or redefined as well as new codes did simultaneously emerge:

- political and diplomatic relations
- the current situation in Russia
- zones of interest
- sanctions
- trade
- proxies
- rhetoric
- academics, and
- social media.

In other words, both an inductive as well as a deductive approach was used.

Reflexive Thematic Analysis (RTA) was developed by Virginia Braun and Victoria Clarke and is an qualitative analysis method that focuses on the researcher as someone who actively provides meanings (Braun and Clarke, 2022). It is a flexible and deeply interpretative approach and is particularly suitable when wanting to understand how people give meaning to their experiences, beliefs, or socio-political realities – which fits well with research on influence, perception, and propaganda. Both a strength as well as one of the downfalls of this methodology is the fact that thematic analysis can be quite subjective.

Analysis: Setting the Stage

A short summary of all seven intelligence reports is:

Denmark

The Danish report outlines a more serious overall threat assessment than they have in many years, or so they mention themselves, and this is due to Russian aggression and its confrontation with the West (Danish Defence Intelligence Services, 2024, p.3). In the eyes of the Danish, Russia has the ambition to enforce a change in the European security order and will intensify its use of hybrid means, including the execution of sabotage actions and malicious influence campaigns. At current there is no threat of a conventional military attack on Denmark, but the military threat from Russia will increase in the coming years as Russia continues to build up its military power. Russia is seen as the most aggressive user of hybrid means. In its report, Denmark, more than other countries, pays attention to developments in the war in Ukraine and poses statements about how it expects the war to unfold in and after 2025. The report does not contain statements that directly relate to public awareness or that emphasise the public duty of the Danish intelligence agency.

Estonia

The Estonian report communicates a grim and urgent picture of the Russian threat, focusing on the ongoing Russian aggression, the spreading of disinformation, and the necessity for the West to act decisively accordingly. The Russian armed forces are rapidly growing and improving on the technological field, particularly in drones, which increases the threat to NATO and Estonia (Estonian Foreign Intelligence Service, 2025, p. 11). Estonia believes Russia may continue its sabotage campaigns in Europe in 2025 to undermine support for

Ukraine, including arson and vandalism. Estonia finds Russia using nuclear weapons is highly unlikely, but it does mention the Russian effort to capitalise on the fear factor to influence Western decision-making. China is involved insofar that it supports Russia by supplying Western components for drones and criticises international sanctions, as a Russian defeat would mean a victory for the U.S. and a setback for China's ambitions. Estonia uses more aggressive rhetoric than other countries and subsequently has the most comprehensive annual report of all. However, Estonia mentions less explicitly than other countries the fact that it is forced to scale up militarily due to the changing security landscape.

Norway

Norway is facing an increasingly challenging security situation, characterised by rising tensions between Russia and China on one side and the West on the other (Norwegian Intelligence Service, 2024, p. 5). Norway argues this situation will lead to an escalation of existing conflicts and to an arms race between great powers. Russia sees itself in direct conflict with the West – a view that remains unchanged regardless of the outcome of the war in Ukraine – and according to Russia, Norway is seen as part of the unfriendly West. Russia is trying to deter Western support for Ukraine through sabotage operations against arms deliveries and critical infrastructure, which could also affect Norway. China and Russia are working more closely together, which has strengthened China's presence and strategic ambitions in the Arctic. Norway on the one hand describes the war in Ukraine in great detail but on the other hardly touches upon topics such as hybrid warfare or propaganda.

Sweden

The security situation in Sweden has deteriorated significantly in recent years (Swedish Armed Forces, 2025, p. 6). The war in Ukraine and the Russian aggression are the most decisive factors in this deterioration. Although Russia's conventional military capabilities in the immediate vicinity of Sweden are currently limited, key capabilities such as naval and air force, cyber capabilities, special forces, and nuclear weapons remain intact. The threat of hybrid warfare has increased, particularly due to Russia's increased willingness to take risks and make use of inexperienced proxies for attacks in Europe. Sweden furthermore places emphasis on the fact that diplomatic relations with Russia have decreased.

Finland

The security situation in Finland is bleak and has significantly changed due to Russia, and there are no signs of improvement – the country states in its report (Finnish Security and Intelligence Service, 2025). Russia is seen as an aggressive, expansionist state that is willing to use all means available to achieve its political goals. The main intelligence threat to Finland comes from both Russia and China. As a result of the war in Ukraine, Russia has become increasingly dependent on China which leads to closer cooperation between the two countries, amongst others in the crucial Arctic region. This includes joint coast guard patrols and military exercises. Russian sabotage operations in Europe have become increasingly dangerous and are aimed at undermining Western support for Ukraine, often through

proxy actors. In its annual report, Finland pays close attention to sanctions evasion and trade relations.

Latvia

In 2024, the aggressive state of Russia remained the biggest threat to the security of Europe, and thus also to Latvia (Latvian State Security Service, 2024, p. 4). In its report, Latvia dedicates an entire chapter to the topic of Counterintelligence. The Russian intelligence and security services (FSB, GRU and SVR) exhibited a high degree of aggression and visibility, its main objectives being the gathering of intelligence and increasing Russia's influence in Latvia. Latvia saw an increase in malicious physical activities, often organized through online communication apps, and carried out by recruits with little training or criminal backgrounds. These activities are aimed at sowing fear and insecurity. The report highlights the role of social media platforms within Russian influence campaigns. The cyber threat from Russia, particularly from hacktivist groups, increased, primarily through DDoS attacks.

The Netherlands

The global unrest and the threat level for the Netherlands and the rest of Europe raises concerns, as the certainties that were previously taken for granted have eroded (Dutch Ministry of Defence, 2025, p. 5). Dutch services expect that the threat from Russia will increase, even after an end to the war in Ukraine. Conflicts are increasingly taking place in the 'grey zone' between peace and war. Russia showed an increased willingness in 2024 to take risks in hybrid attacks, including a cyber-sabotage attack on a digital control system of a public utility in the Netherlands and preparing sabotage

activities against critical infrastructure in the North Sea. China also poses a threat through its support of Russian warfare and its aggressive stance towards Taiwan.

Coding Scheme

This section outlines the three concepts of intelligence communication as outlined by Petersen (2019) and presents an overview of the thematic structure.

Awareness

"The first concept of communication as awareness is (...) not aimed at spurring civil action or mobilizing the public to the management of new threats. Rather, this conceptual discourse describes communication as a means to create accountability in the institutions by creating a general democratic public awareness." (Petersen, 2019, p. 319)

In the first communication strategy, the intelligence agency informs the public about threats, risks, or strategic trends without explicitly calling for action. This may include:

a) a description of Russian threats (cyber, hybrid, espionage, nuclear or sabotage),

b) an explanation of geopolitical contexts (such as China, Iran, Belarus, the Arctic),

c) the monitoring of threat levels or trends, or

d) a chronological overview of incidents or threats.

Table 1. Awareness in selected countries

Country	Quote	
Denmark	"In the current situation, it is less likely that Russia is intent on launching destructive cyber-attacks against Denmark in which the purpose is to create serious and far-reaching consequences for critical societal functions."	a
	"The war in Ukraine has now lasted for almost three years, and its consequences are increasingly being felt here in Denmark. The threat of Russian sabotage has increased, especially against targets linked to Danish support for Ukraine, as has the threat of serious Russian cyber-attacks."	a,c
Estonia	"Should the war in Ukraine end favourably for Russia, or if hostilities are frozen, it is almost certain that Russian military units will be permanently stationed along Estonia's borders in greater numbers than before 24 February 2022."	c
	"Russia is highly unlikely to use nuclear weapons in its war against Ukraine and instead seeks to maximise its fear factor to sway Western decision-making. Russia's nuclear threats have not yielded the desired results, and this is causing frustration among the country's leadership."	a
Finland	"Finland has not been a target of strong Russian influencing so far. Such influencing has instead primarily target large EU Member States, and also countries with a substantial Russian minority or pro-Russian political parties."	a
	"As relations between Russia and the West have cooled, Russian influencing has grown more severe. Russian sabotage operations in Europe may be viewed as one aspect of this."	c

Latvia	"Traditional intelligence activities – recruiting Latvian nationals for prolonged and secret collection of information – will remain the basis for operation of Russia's intelligence and security services."	a
	"The significance of the messaging application 'Telegram' in supporting Russia's interests continues to increase: currently this platform provides unlimited possibilities not only to disseminate pro-kremlin narratives, but also to recruit participants for operations inspired by Russia's intelligence and security services."	a,c
Netherlands	"Our country is being increasingly confronted by hybrid attacks by state actors in an attempt to disrupt and weaken our society. Russia in particular is mounting cyber-attacks while aiming to remain below the threshold of armed conflict, although an increased willingness to take risks has been perceived."	a,c
	"Russia took a number of concerning steps towards escalation in 2024. For example, the publication of the revised Nuclear Doctrine (with a further lowering of the nuclear threshold), the first ever employment of an intermediate range ballistic missile (whose primary task is nuclear), and statements that Russia is prepared to resume nuclear testing are all intended to generate uncertainty."	c,d
Norway	"The shadow fleet undermines sanctions and safe shipping, and presents a challenge to Norway."	a
	"The expulsion of Russian intelligence personnel from European countries has compelled Russia to make more frequent use of proxies in covert operations in Europe. These proxies conduct influence operations, political subversion, sabotage	a

	and information gathering on behalf of Russian state actors."	
Sweden	"Russia has announced that a number of measures will be taken to counter the perceived deterioration of the security policy situation experienced in the Swedish vicinity. The measures are mainly long-term and aim to strengthen conventional military capabilities by reorganising the military zones in western Russia."	a
	"It is clear that the Russian leadership considers the question of Russia's greatness and place in the world to be far more important than the welfare of its people."	a

Advice

> *"Where this first concept of communication ('communication as awareness') tends to assume a subtle and historically bound relation between the agency and the public, (...) the second concept ('communication as advice') designates the public as an agent that can act on the requests of the agency. We thus turn from a discourse of democratic openness and awareness, to one on effectiveness and action,"* (Petersen, 2019, p. 320)

When using this second communication strategy, an intelligence agency gives direction to the behaviour of citizens, businesses or institutions through explicit recommendations or implicit warnings. This can include:

a) warnings for the commercial sector about sanctions or the export of certain products,

b) recommendations for governmental or military readiness,

c) calls for vigilance or the strengthening of defensive measures, or

d) policy suggestions regarding cyber resilience or one's information position.

Table 2. Advice in selected countries

Country	Quote	
Denmark	N.a.*	
	N.a.	
Estonia	"Western nations largely recognise the security risks posed by Russian state media and have significantly curtailed their influence through sanctions. A similar approach should be applied to Russian 44 think tanks operating in the West."	b,c
	"The National Security Authority within the Estonian Foreign Intelligence Service supports companies in navigating classified information protection requirements for projects."	c
Finland	"Russia's emphasis on an imperialist character, factually unfounded historical interpretations, and a decades-long manipulation of the nation into believing in the historic mission of the country, call for a capable and strong Finnish intelligence that can provide early warning of potential measure against Finland."	b
	"Enterprises are required to know the parties with whom they transact business. They are ultimately responsible for verifying the final destination of the products that they sell. All enterprises and private	a

	operators should be aware of the risks involved in circumventing sanctions and export restrictions. Corporate management is criminally liable for complying with EU sanctions and export restrictions."	
Latvia	"VDD (Valsts Drošības Dienests, the Latvian State Security Service) stresses to all members of society that in such cases it is crucial to react as fast as possible, duly register the suspicious incident – preferably also by photo or video – and immediately report the incident to the State Police by calling 110.	c
	"The transport sector will continue to face the current challenges related to decrease in cargo turnover and necessity to reorient from the former intense cooperation with Russia and Belarus to new sources of cargo flows."	a
Norway	"Risiko", NSM's (Nasjonal Sikkerhetsmyndighet, Norwegian National Security Authority) annual risk assessment, aims to help Norwegian enterprises manage security risks by providing information about vulnerabilities, threats and security measures."	b
	N.a.	
Netherlands	"The Dutch services believe that the threat posed by Russia to Europe will grow rather than diminish, even if the war in Ukraine is brought to an end. This underlines the importance for the Netherlands, for NATO and particularly for the EU member states to build up military striking power as quickly as possible."	c
	"DISS has been warning about this cyber threat for some time. For example, in the past year DISS (Defence Intelligence and Security Service) publicised the working methods of a Russian GRU	a

	unit in order for potential victims to arm themselves against serious attacks of this nature and against espionage."	
Sweden	"In order to increase the capability of our total defence, it is of great importance that Sweden addresses the threats to our society with a coordinated approach. Action needs to be taken by different actors at different levels, both public and private."	b
	"The military threat requires a continued rapid increase in military defence capabilities."	c

* N.a. = Not applicable.

Co-Production

> *"While the concept of communication as advice enforced a clear separation between sender and receiver, this third concept of communication (as co-production) goes beyond such an understanding of communication and challenges the boundary of the institution. In a broader historical perspective, one could argue that this turn to 'communication as co-production' reflects a shift from government to governance, from a centralized to a decentralized understanding of security expertise. In other words, it recognizes the importance of security management being made outside the jurisdiction of nation-state bureaucracies, in a fragmented public and private sphere. The emphasis is on social networks, professional networks, economic and even criminal networks, tightly or loosely organized in communities of knowledge."* (Petersen, 2019, p. 322)

An intelligence agency that uses the third strategy might argue that security is partly dependent on the actions of citizens, businesses, and/or other societal institutions. A shared responsibility is stated or implied. This can include:

a) references to 'total defense', resilience and cooperative responsibility,

b) encouragement for alertness or collaboration amongst public actors, or

c) explicitly laying responsibility with companies (such as compliance with sanctions) or citizens.

Table 3. Co-Production in selected countries

Country	Quote	
Denmark	N.a.	
Estonia	"Russian special services actively seek access to critical information of their perceived enemies, both classified and unclassified. Protecting electronic information requires the methodical use of robust, independently evaluated cryptographic solutions. Post-quantum cryptography should already be adopted to address emerging threats from quantum computing."	c
Finland	"Businesses may be unwittingly involved in circumventing sanctions and export restrictions as Russian procurement routes become more complex and increasingly linked to the EU internal market. Enterprises should always pay particular attention to unusual procurement efforts or contacts."	c
	"National authorities need the expertise of academic institutions, private enterprise and specialists to succeed in a continually evolving cyber world. The	a

	combined capacities and capabilities of various actors in complex networks is called a cyber ecosystem."	
Latvia	"VDD highly values the engagement of society in identifying suspicious activity and threats and regularly reporting them to VDD. The participation of every member of society in strengthening national security remains crucial."	c
Norway	N.a.	
Netherlands	"DISS works in an ecosystem together with the private sector and knowledge institutions on the latest technologies, products, services and expertise. Strengthening these partnerships forms an important part of our vision for the future."	a
Sweden	"Countries whose societal model is based on democracy, the rule of law, civil society and the market economy are thus facing systemic confrontation. This requires society as a whole to have the capacity to coordinate across administrative boundaries in order to address a wide range of threats without compromising fundamental values."	a

Beyond Awareness, Advice and Co-Production

The comparative analysis of the seven intelligence reports shows how different agencies position themselves institutionally through their public communication strategies. Some primarily assume an informative role, presenting themselves as monitors of threats and custodians of situational awareness, while others move further towards an advisory or collaborative stance, framing citizens, companies, and institutions as active security partners. These choices reflect

organisational preferences as well as broader national security cultures and traditions of state- society relations.

The Nordic countries demonstrate variation in emphasis. Denmark and Norway remain relatively restrained, largely limiting their role to situational reporting and the provision of background awareness. They present themselves as state institutions that observe and warn, with little expectation of direct citizen involvement. Sweden and Finland, by contrast, articulate more explicit calls for readiness and resilience. Sweden stresses the need for a '*total defence*' approach that mobilises different sectors of society, while Finland frequently points to sanctions compliance, vigilance against recruitment, and the necessity of joint public–private expertise in cyber defence. Finland hereby recognises the shared responsibility and the 'need to share' culture which Petersen refers to in her article (Petersen, 2019, p. 319). These differences suggest that while Nordic agencies share a concern with hybrid and conventional threats, their communication styles diverge between a state-centred, informative model and a societal resilience model.

The Baltic States adopt a more urgent and interventionist tone, which reflects their immediate exposure to Russian pressure. Both Estonia as well as Latvia combine stark awareness-raising with advisory and co-productive elements. Latvia explicitly stresses public participation in identifying and reporting threats. Its report reveals an institutional role conception in which intelligence is not confined to professional agencies but embedded in broader networks of societal actors. Estonia also frames security as contingent on cryptographic and mathematics innovation and business compliance but places the

responsibility for this with the Estonian National Security Authority, part of the Estonian Foreign Intelligence Service – which is illustrative of the fact that it still tends to view security as largely a governmental matter.

The Netherlands balances between awareness and advice, with a strong emphasis on monitoring hybrid, cyber, and nuclear-related threats. Its intelligence agency warns about the persistence of Russian grey-zone activities and calls for strengthened military capabilities at the national and European level, underlining a primarily informative and advisory role. At the same time, the report refers to working in an '*ecosystem'* with private and knowledge sectors, signalling a selective co-productive element. Compared to the Baltic states, however, this collaborative framing is less pronounced and functions more as a supplement to the agency's core emphasis on awareness and warning.

Across these cases, the differences in communication strategies are not only institutional choices but also reflect wider policy orientations. As pointed out in the introduction, recent scholarship has drawn attention to the growing adoption of a whole-of-society approach to security in Europe (Jermalavičius & Parmak, 2014, p. 24). This framework conceives of resilience as a shared mission, extending responsibility for national defence beyond state institutions to include civil society, private sector actors, and the wider public (Wigell, Mikkola & Juntunen, 2021, p. 19). It has been applied in areas such as hybrid-threat response, total defence, and disinformation resilience (Zdanavičius & Statkus, 2020, p. 1). Seen from this perspective, the movement of some intelligence agencies from an exclusive focus on

awareness towards advice and co-production can be read as part of this broader trend. Public communication thus acquires a new function: not only to provide transparency, but also to grow awareness and strengthen social resilience against external disruption.

Conclusion

Intelligence communication is not just reactive; it is strategic (NATO, 2025b, p. 6). Similarly, annual threat assessments are not merely informational – they are strategic instruments that frame and shape adversarial behaviour, signal national resolve and cultivate public resilience.

All seven countries apply the strategy of 'Awareness' in their communication, and with the sole exception of Denmark, also the strategy of 'Advice'. The public is not only informed about threats and risks but is also given specific directions of behaviour through explicit recommendations or implicit warnings. The strategy which Petersen calls 'Co-Production' is not in all reports visible, and with varying degrees of explicitness. The whole-of-society approach, which is already being used often in policy circles, is not as much reflected in practice as one might have thought. While there is a trend of intelligence organisations in Western democracies intensifying their communication strategies, the extent to which their annual threat assessments and public reports embody the principles of broad societal engagement, is incongruent. As it is a conscious choice of intelligence agencies to adopt this approach or not, it is interesting to conclude that many European intelligence agencies have not (yet) made this choice. Of the seven states examined, the Baltic States

are most forward leaning which can be explained by their immediate exposure and vicinity to Russian pressure. Next in line are Finland and Sweden.

Nevertheless, beyond the researched intelligence agencies and their annual reports a gradual trend is emerging in which intelligence agencies step out of the shadows to show they are part of society, while also projecting capability and discrediting adversaries. Ukraine's military intelligence directorate (GUR) is illustrative: its leadership is visible in the media, it organises crowdfunding initiatives and public events, and it offers hotlines and chatbots for citizen interaction (Schrijver, 2024). Similar dynamics are evident in Israel and the United Kingdom, where intelligence agencies use communication to justify operations and project credibility. By contrast, as observed in this research, many European agencies remain more reserved, limiting their public role to formal threat assessments and avoiding broader societal engagement, despite calls for whole-of-society approaches as an answer to the Russian threat.

Literature:

1. Aldrich, R.J., & Moran, C.R. (28 March 2018). 'Delayed Disclosure: National Security, Whistle-Blowers and the Nature of Secrecy', Political Studies, 25. https://doi.org/10.1177/0032321718764990.
2. Akrap, G., Mandić, I., & Žigo, I.R. (05 Oct 2022). 'Information Supremacy, Strategic Intelligence, and Russian Aggression against Ukraine in 2022', International Journal of Intelligence and Counterintelligence, 36. https://doi.org/10.1080/08850607.2022.2117577.

3. Avidar, R., & Magen, C. (2023). 'Negative Spaces as a Strategic Decision: The case of the Israeli Security Agency.' Public Relations Review, 49, 2, 102315.

4. Braun, V., & Clarke, V. (2022). Thematic Analysis: A Practical Guide. London: SAGE.

5. Danish Defence Intelligence Service (2024). Intelligence Outlook 2024. Retrieved from https://www.fe-ddis.dk/globalassets/fe/dokumenter/2024/intelligenceoutlook.pdf.

6. Dutch Ministry of Defense (2025). Public Annual Report 2024. Retrieved from https://www.defensie.nl/downloads/jaarverslagen/2025/04/22/public-annual-report-2024-netherlands-defence-intelligence-and-security-service.

7. Doyle, M.W. (1983). 'Kant, Liberal Legacies, and Foreign Affairs', Philosophy and Public Affairs, 12, 3, 205-235.

8. Dylan, H., & Maguire, T.J. (2022). 'Secret Intelligence and Public Diplomacy in the Ukraine War', Survival 64, 4 (2022): https://doi.org/10.1080/00396338.2022.2103257 .

9. Estonian Foreign Intelligence Service. (2025). International Security and Estonia 2025. Retrieved from https://www.valisluureamet.ee/doc/raport/2025-en.pdf.

10. Finnish Security and Intelligence Service. (2025). SUPO National Security Overview 2025. Retrieved from https://katsaus.supo.fi/en/frontpage.

11. Gill, P., & Phythian, M. (2018). 'Developing Intelligence Theory', Intelligence and National Security 33, 4. https://doi.org/10.1080/02684527.2018.1457752 .

12. Hulnick, A.S., (1999). 'Openness: Being Public About Secret Intelligence', International Journal of Intelligence and CounterIntelligence 12, 4. https://doi.org/10.1080/ 088506099305007 .
13. Jermalavicius, T., & Parmak, M. (2014). Societal Resilience: A Basis for Whole-Of-Society Approach to National Security. National Security.
14. Krotz, F., (2017). 'Explaining the Mediatisation Approach', Javnost - The Public 24, 2: 103, https://doi.org/10. 1080/13183222.2017.1298556.
15. Landon-Murray, M. (2015). Social Media and U.S. Intelligence Agencies: Just Trending or a Real Tool to Engage and Educate? Journal of Strategic Security, 8, 3, 67-79.
16. Latvian State Security Service. (2024). Annual report 2024. Retrieved from https://vdd.gov.lv/en/useful/annual-report-2024.
17. Magen, C. (2017). 'Strategic Communication of Israel's Intelligence Services: Countering New Challenges with Old Methods', International Journal of Strategic Communication, 11, 4.
18. McLoughlin, L., Ward, S., & Lomas, D.W.B. (2020). 'Hello, world': GCHQ, Twitter and social media engagement'. Intelligence and National Security, 35, 2. https://doi. org/10.1080/02684527.2020.1713434
19. NATO. (2025a). 'Joint Press Statements by NATO Secretary General Mark Rutte with the Prime Minister of Portugal, Luís Montenegro, NATO, accessed 7 February 2025, https://www.nato.int/cps/en/natohq/opinons232562.htm.
20. NATO. (2025b). Intelligence and Strategic Communication. NATO STRATCOM COE.
21. Norwegian Intelligence Service. (2024). FOCUS 2025. Retrieved from

https://www.etterretningstjenesten.no/publikasjoner/fokus/focus-in-english/Focus2025%20-%20EN%20-%20Printer-friendly%20v3.pdf.

22. Petersen, K.L. (2019). 'Three Concepts of Intelligence Communication: Awareness, Advice or Co Production?' Intelligence and National Security, 34, 3: 317-28, https://doi.org/10.1080/02684527.2019.1553371.
23. Pew Research Centre (2015, November 23). Beyond Distrust: How Americans View Their Government. https://www.pewresearch.org/politics/2015/11/23/1-trust-in-government-1958-2015/.
24. Riemer, O., & Sobelman, D. (2023). 'Coercive Disclosure: The Weaponization of Public Intelligence Revelation in International Relations', Contemporary Security Policy 44, 2. https://doi.org/10.1080/13523260.2022.2164122.
25. Schrijver, P. (2024). 'From the Shadows to the Social Sphere: Ukraine's Strategy of Engagement', Irregular Warfare Initiative. Retrieved from https://irregularwarfare.org/articles/from-the-shadows-to-the-social-sphere-ukraines-strategy-of-engagement/.
26. Schrijver, P., Nietzman, L., & Pijpers, P.B.M.J. (2025). 'Birdwatchers on Social Media: The Mediatisation of Intelligence Organisations', Security and Defence Quarterly, 49, 1: 1-21, https://doi.org/10.35467/sdq/196516.
27. Strömbäck, J., & Esser, F. 'Mediatization of Politics: Transforming Democracies and Reshaping Politics', in Mediatization of Communication, by Knut Lundby (De Gruyter,

2014), 374, WorldCat, https://doi.org/10.1515/9783 110272215.375.

28. Swedish Armed Forces. (2025). MUST Annual Report 2024. Retrieved from https://www.forsvarsmakten.se/contentassets/546bbe13064a4c739e1cbc4b5e4571f7/2024-must-annual-report.pdf.
29. Ukrainian World Congress, 'Landsbergis: West Ignored Baltic Countries' Warnings about Russia', accessed 7 February 2025, https://www.ukrainianworldcongress. org/former-lithuanian-minister-west-ignored-baltic-countries/warnings-about-russia/.
30. Van Puyvelde, D., (2013). 'Intelligence Accountability and the Role of Public Interest Groups in the United States'. Intelligence and National Security 28, 2: https://doi.org/10.1080/02684527.2012.735078;
31. Wigell, M., Mikkola, H., & Juntunen, T. (2021). Best Practices in the Whole-of-Society-Approach in Countering Hybrid Threats. European Parlement. Retrieved from https://www.europarl.europa.eu/RegData/etudes/STUD/2021/653632/EXPO_STU(2021)653632_EN.pdf.
32. Williams, P.D., & McDonald, M. (2023). Security Studies: An Introduction. New York: Routledge.
33. Yanchenko, A. O., 'Mediatisation and Self-Mediation of Political Participation: New Citizenship Practices and Social Media', Visnyk of the Lviv University, 2021, 277, https://api.semanticscholar.org/. CorpusID: 2397492 56.
34. Zdanavicius, L.,, & Statkus, N. (2020). Strengthening Resilience of Lithuania in an Era of Great Power Competition: The Case for Total Defence. Journal on Baltic Security, 6, 2. https://doi.org/10.2478/jobs-2020-0009

35. Zegart, A., & Morell, M. (2019). Spies, Lies, and Algorithms: Why U.S. Intelligence Agencies Must Adapt or Fail. Foreign Affairs 98, 3.

36. Zeitzoff, T. (2017). 'How Social Media is Changing Conflict', Journal of Conflict Resolution 61, 9, https://doi.org/10.1177/0022002717721392.