PRIO

Independent • International • Interdisciplinary

PRIO PAPER 2026

# Increasing resilience in the age of disinformation

*Recommendations for enhanced preparedness through collective psychological defence*


Stine Bergersen
*Peace Research Institute Oslo (PRIO)*

Gabriel Lönn
*Peace Research Institute Oslo (PRIO)*

Peace Research Institute Oslo (PRIO)
PO Box 9229 Grønland, NO-0134 Oslo, Norway
Visiting Address: Hausmanns gate 3

www.prio.org
Facebook: PRIO.org
X: PRIOresearch

ISBN: 978-82-343-0737-9 (print)
978-82-343-0738-6 (online)

Cover: Getty Images

# Increasing resilience in the age of disinformation

Recommendations for enhanced preparedness through collective psychological defence

Stine Bergersen
*Peace Research Institute Oslo (PRIO)*

Gabriel Lönn
*Peace Research Institute Oslo (PRIO)*

Peace Research Institute Oslo (PRIO)
Hausmanns gate 3
PO Box 9229 Oslo
NO-0134 Oslo, Norway
Tel. +47 22 54 77 00
www.prio.org

PRIO encourages its researchers and research affiliates to publish their work in peer-reviewed journals and book series, as well as in PRIO's own Paper and Policy Brief series. In editing these series, we undertake a basic quality control, but PRIO does not as such have any view on political issues. We encourage our researchers actively to take part in public debates and give them full freedom of opinion. The responsibility and credit for the hypotheses, theories, findings and views expressed in our publications thus rest with the authors themselves.



ISBN: 978-82-343-0737-9 (print)
ISBN: 978-82-343-0738-6 (online)

Cover design: www.medicineheads.com
Cover photo: Getty Images

# Contents

# List of figures



# List of tables

# 1. Executive summary

The continuous exploration of how democratic societies can best be protected against disinformation, while preserving fundamental freedoms, is more relevant than ever. The issue is central to maintaining trust in public institutions and ensuring an open and democratic society, while managing complex threats in a complex context. The World Economic Forum, in their 2026 Global Risks Report (2026), ranked misinformation and disinformation as the second biggest global risk by severity in the next two years (with geoeconomic confrontation ranked first) (World Economic Forum, 2026). In the 2025 report, it was ranked first, implying that disinformation was considered a more serious threat than both extreme weather events and state-based armed conflicts (Elsner et al., 2025).

This PRIO Paper provides the Norwegian Ministry of Defence (MoD) with a knowledge-based approach for enhancing public understanding of the threat landscape, drawing on what are considered core principles of psychological defence. Psychological defence refers to strategies, capabilities and societal resilience measures designed to protect populations against foreign influence operations and hybrid threats, including disinformation, propaganda and cognitive manipulation (Palmertz et al., 2024). The report concludes by delivering a set of recommendations aimed at increasing public resilience in a new age of security policy where hybrid threats such as disinformation proliferate.

Concretely, the research project on which this PRIO Paper is based answered three central questions:

1. Drawing on existing knowledge,[1] what do current approaches for increasing public resilience to disinformation look like in European contexts, other than Norway?
2. In the Norwegian context, what is the potential of the concept of psychological defence as a way of advancing public knowledge about the threat of disinformation?
3. Based on the insights derived from the above research questions, what are the key recommendations for the Norwegian Ministry of Defence?

Answering the final question, the report presents recommendations and issues for future consideration. One conclusion is that a **whole-of-society approach** is needed to counter and prepare for hybrid threats, including disinformation. Importantly, psychological defence is not just about countering propaganda but about building societal resilience. Traditional countermeasures like fact checking and increasing media literacy are important, but insufficient, since **disinformation often works by undermining trust, not just by spreading false information**.

Another insight is that thinking along the lines of a national psychological defence (referring to the Swedish model with the Psychological Defence Agency) shifts the focus from correcting individual claims to strengthening cognitive and emotional resilience, which on the individual

level can help people recognize manipulation and be better equipped to resist the adverse effects of disinformation. On the societal level, **stronger national coordination is needed** to manage efforts to build resilience. This would help create a better defined space for targeted efforts at resilience building. This, in turn, can contribute to building and maintaining trust in democratic institutions.

Related to coordination, this report also emphasizes the importance of deliberation among all involved stakeholders and decision-makers when it comes to **concepts and terminology**. In other words, the language used to describe the phenomena central to this report is crucial for how they are dealt with and understood.

Furthermore, the report highlights **public awareness initiatives**, as well as trust-building and trust-maintenance. It concludes that strategic communication is increasingly important for national authorities, to build trust also outside of crisis. This is especially important if the MoD considers the *will* to defend as central to the *ability* to defend. **Strategic communication from national authorities** less public facing such as the MoD and the Norwegian Intelligence Service of the Armed forces is particularly viable as a way of strengthening public resilience to disinformation.

Finally, building resilience to disinformation requires a **holistic approach**. Any efforts to increase resilience to disinformation should be organized in a way that not only considers shifting (geo)-political, social and cultural contexts, but also underscores the democratic values which are in fact threatened by disinformation.

# 2. Introduction

The Commission on Freedom of Expression (*Ytringsfrihetskommisjonen*), the Total Preparedness Commission (*Totalberedskapskommisjonen*) and the Defence Commission (*Forsvarskommisjonen*) all emphasize that the most important measure against complex threats, influence operations and disinformation is a resilient Norwegian society. Trust, along with an open and informed public discourse, is central to ensuring this. As described also in the Strategy to Strengthen Resilience against Disinformation (2025–2030) (*Strategi for å styrkje motstandskrafta mot desinformasjon (2025–2030)*), a comprehensive approach to disinformation can be divided into four phases: prevent, detect, respond and evaluate. In the current report, we focus mainly on the first phase, where the underlying assumption is that preventing or limiting the adverse effects of disinformation involves strengthening societal resilience.

The impact of disinformation on an open democratic society like Norway depends on how we respond to it. Research shows that while it is difficult to prevent the spread of disinformation, a more suitable approach may be to try to limit the effect it has on the recipient, i.e. the public (Sivertsen et al., 2021: 35). Preventing the existence, emergence and spread of disinformation is a different task than preventing or limiting the damaging *consequences* it can have on society and individuals. This report, and its recommendations, aims to contribute to the latter.

## 2.1. On disinformation

Disinformation is often defined as the creation and spread of deliberately false information with harmful intentions. According to a recent report by The European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE), 83% of the Hybrid CoE's Participating States and Organisations agree or strongly agree that disinformation is a significant threat to national security (Kalenský & Hanhijärvi, 2025: 9). In the same survey, 48% state that their country does not have a dedicated strategy in place to counter disinformation, and 59% state that their country does not have a dedicated government agency in place to counter disinformation (Kalenský & Hanhijärvi, 2025: 10). Less than half of the respondents evaluate their government's response to disinformation as well-communicated and transparent to the public (Kalenský & Hanhijärvi, 2025: 12). This suggests that there is room for improvement.

Disinformation increasingly plays a role in attacking public morale by targeting general populations and eroding societal trust in both the state and national institutions (Filipec, 2019). Disinformation is an efficient weapon for destabilizing societies and making them less robust in the face of hardship, both in times of peace and in moments of war. There is little room for doubt that foreign actors engaging in manipulation of public opinion by spreading false information are a real threat. Internationally, several high-profile cases highlight the dangers: In Myanmar, information shared on Facebook was found to be a factor in causing the Rohingya Genocide, and online propaganda by the ruling Bharatiya Janata Party (BJP) party in India relies on large-scale video and image manipulation, to cast minority groups in a bad light. In the US,

but consequentially also elsewhere, the public debate around disinformation was amplified during two major events: the US 2016 presidential election and the so-called Cambridge Analytica scandal. Regarding the former, disinformation played a central role during the election, with coordinated efforts, particularly by Russian state-linked actors, to influence public opinion, deepen divisions and undermine trust in democratic institutions in the US. It was later confirmed in the Mueller Report that the Internet Research Agency (IRA), a Russian 'troll farm', carried out large-scale disinformation campaigns across social media platforms, where content was tailored to exploit societal divisions on race, religion, immigration, gun rights and more. Regarding the latter, the Cambridge Analytica scandal was a data privacy and political controversy that came to light in 2018, involving the harvesting of personal data from millions of Facebook users without their consent and used to influence elections.

The European security situation is currently tense, with ongoing wars in both Ukraine and in Gaza. The impact on Norway is unquestionable. For example, the Norwegian Intelligence Service of the Armed Forces (NIS) underline in their national threat assessment report in 2024 that Norway is indeed considered a relevant target of political manipulation, in particular by Russia. Influence operations are part of Russia's information warfare, and singling out specific target groups on social media for pro-Russian messages and disinformation is a typical method. Another course of action is to plant different theories and lies about a specific matter in order to obfuscate reality and undermine public trust in the authorities and national media (NIS, 2024). At the same time, NIS emphasize that increased vigilance in the Western population combined with greater distrust of Russian intent have created challenges for Russian influence actors. Although extremist and anti-government groups that rely more on informal media are currently more exposed to Russian influence activity than society at large, pro-Russian 'hacktivists' have also carried out denial-of-service attacks against Norwegian targets. Part of the purpose of such attacks is, according to NIS, to sow doubts about the ability of Norwegian institutions to provide services, thereby influencing public trust in authorities. As per the 2024 report, this activity has had limited effect beyond attracting public attention, but new attacks are likely in the coming years (NIS, 2024).

## 2.2. On resilience

In Norway, there is still ample space for further developing and improving resilience (Bergaust et al., 2022: 4). Resilience can be defined as an ongoing sensemaking process that relies on communicative interactions to understand and respond to a given adversity (Anderson & Guo, 2021). For example, creating resilience can imply enabling adaptation to change or difficult circumstances, by providing the appropriate tools. The prevalence of disinformation means that finding strategies and tools for strengthening society's collective adaptability is key. In both policymaking and academia, there is therefore a growing recognition of the relevance of societal trust and resilience for national security and crisis management (Ridley, 2017; Meld. St. 5 2020–2021; NOU 2023:17).

In Norway, the combination of the total defence concept, the proliferation of advanced emerging technologies (including AI and algorithmically-driven digital platforms) and increased global interconnectivity points to some challenges. A better understanding of disinformation and its actual and potential effects becomes transversally important; as the threats change, so must our responses. And Norwegian authorities indeed recognize that disinformation, which is expected to increase in both volume and intensity, threatens to weaken the population's ability and willingness to defend Norway. This drives the necessity to increase public awareness and knowledge about defence and emergency preparedness (NOU 2023:14: 95).

## 2.3. On psychological defence

As a way of building resilience, and to limit or lower the risks created by foreign intervention in public discourse and communication, the concept of psychological defence (as defined by the Swedish Psychological Defence Agency) focuses on making individual citizens aware that they could be exposed to influence from foreign powers and providing them with tools for how to detect and manage such influence. To counter malign influence aimed at changing people's perceptions or influencing their behaviours, a coordinated psychological defence effort acknowledges that the first line of defence consists of source-critical individuals. Although Norway does not have a dedicated agency responsible for this task, Norwegian authorities recognize that critical media literacy, the population's ability to exercise source criticism and recognize false information, is considered part of societal resilience (Meld. St. 9 (2022–2023): 16). However, as this PRIO Paper will explore, resilience to disinformation goes beyond fact checking and media literacy.

The 'Increasing resilience in the age of disinformation' project leading up to this report is based on the acknowledgement that ensuring high situational awareness in the public must be included in the broader defence and emergency preparedness work. As stated earlier, the report responds to three central questions:

1. Drawing on existing knowledge, what do current approaches for increasing public resilience to disinformation look like in European contexts, other than Norway?
2. In the Norwegian context, what is the potential of the concept of psychological defence as a way of advancing public knowledge about the threat of disinformation?
3. Based on the insights derived from the above two research questions, what are the key recommendations for the Norwegian Ministry of Defence?

The concluding recommendations and issues to consider are aimed at increasing public resilience in a new age of security policy where hybrid threats such as disinformation proliferate.

## 2.4. Data collection and methods

To explore the research questions, various methods were employed, including document analysis and literature review, as well as semi-structured interviews with some key actors and stakeholders. A list of some key data collection activities is included below.[2]

- Meeting at PRIO with Major General Oleksii Migrin, Deputy Head of SESU (State Emergency Service Ukraine), Colonel Viktor Vitovetskyi, Director of the Civil Protection Department and Serhii Kravchenko, Senior Lieutenant of the International Cooperation Department at SESU (translator).
- Interview with Andreas Skjøld Lorange, Specialist Director at the National Security Authority (NSM).
- Interview with General Director Magnus Hjort of the Swedish Agency for Psychological Defence (*Myndigheten för psykologiskt försvar* – MPF).
- Participation at the *Cognitive Warfare and Security workshop* (as part of the CENTREPEACE project), Helsinki, May 2025.
- Participation (by invitation only) at the 2025 *Oscarsborg Symposium on Nordic Security: Communicating for war and countering disinformation: The Nordic approach*, 2–3 October 2025. The symposium gathered key leaders, experts and scholars across sectors and countries to discuss communication on war preparedness and managing disinformation. The symposium was held under Chatham House rules, meaning that the content of the presentations and discussions are referred to in this report without attribution to any individual or organization.
- Participation at the Total Defence Conference (*Totalforsvarskonferansen 2025*) in Oslo, April 2025.
- Participation at the Vulnerability Conference 2025 (*Sårbarhetskonferansen 2025*) in Oslo, September 2025.
- Participation at the *Words! Matter 2025* conference by the Oslo Center. The conference examined collective responsibilities to challenge disinformation and the importance of re-building trust in a fractured world. It aimed at identifying where responsibility lies across government, business and religion – as well as the next generation.
- Participation at the launch of the new national strategy for increasing resilience to disinformation by the Norwegian Ministry of Culture and Equality, June 2025.

In addition, this report reflects the findings of a national two-part survey carried out in relation to the research project *Disinformation and people: impacts on societal trust and resilience*, led by the Arctic University of Tromsø, in collaboration with PRIO and others.

For The 'Increasing resilience in the age of disinformation' project, the research project that produced this report, the project leader met with representatives from the MoD to discuss the project and to receive some insights in March 2025. The project was carried out in two parts: the first part consisted of desk research and literature review and took place between March 2024 and May 2024, and the second part consisted of data collection (via interviews) and further research that took place between February 2025 and November 2025. An internal working paper version of the report was submitted to the Norwegian Ministry of Defence in November 2025, and the final version was submitted in April 2026.

During the research process, the topic of disinformation has become even more relevant and has continued to challenge public institutions, the defence sector and ordinary citizens. While underlining the report's salience, these developments have also required the exclusion of some developments. For example, an important distinction is made between measures to counter disinformation, and measures to increase resilience to disinformation, where the former mainly implies efforts targeted against the actors creating and sharing disinformation, while the latter implies efforts aimed at the public, which is what the report deals with. The report also does not cover analysis of the specific legal environments. Also, the choice to focus primarily on the Swedish context was made, both because of its uniqueness in the European context, granting it comparative potential, and because Sweden has taken a leading role in institutionalizing psychological defence. A closer analysis of the Swedish case meant that less resources were spent on the description of other contexts. Additional knowledge on European contexts and approaches is nonetheless covered in other reports, such as those by Bergaust et al. (2022), Freihse & Bochert (2024), Lindgren et al. (2026) and Kalenský & Hanhijärvi (2025).

After this chapter, which introduces the report and its methods, the rest of the report is structured as follows:

- **Chapter 3: Concepts and contestation** deals with the central concepts of the report: resilience, disinformation (and related concepts) and psychological defence. This includes a state-of-the-art presentation of such terms from the research and policy fields, and the different meanings they have in different disciplines and institutional settings. This chapter explores the contestations surrounding the concepts themselves, while also underlining the importance of semantics more fundamentally.
- **Chapter 4: Resilience and defence against disinformation: Norwegian and European approaches** deliberates on increasing resilience to disinformation in peacetime versus war, in Norway and in the EU. It also presents some insights from France, Finland and Ukraine.
- **Chapter 5: The Psychological Defence Agency (MPF) in Sweden** provides an overview of the agency in terms of organizational structure, funding, governance, mandate and

rationale. It also goes into some detail on a case where the operations department of the MPF countered a disinformation campaign which first emerged between 2022 and 2024, in association with Sweden's accession to NATO, the so-called 'LVU campaign'.

- **Chapter 6: Analysis and findings** builds on the state-of-the-art on terms and concepts in Chapter 3, and presents a section on research on resilience and disinformation. It then presents some insights from a two-part survey designed to better the understanding of public perceptions, trust and behaviours around disinformation in Norway. The chapter summarizes some of the main differences between the Norwegian and Swedish approaches to institutionalizing resilience and focuses on real and potential challenges, drawing on some lessons learned from Sweden. It also provides a summary of what we see as main challenges and opportunities.
- **Chapter 7: Recommendations for strengthening societal resilience against disinformation** concludes with recommendations and suggested focus areas, which are, based on the research done in this context, considered relevant for strengthening resilience against disinformation in Norway. The report ends with some additional suggested reflection points.

# 3. Concepts and contestations

The central concepts of this PRIO Paper are both contextual and fluid, in the sense that their content and meaning continue to vary, across countries and across sectors. However, this report importantly also acknowledges and highlights some inherent difficulties in defining such concepts. As the report will show, efforts to define and delimit the concept of disinformation, in particular, comes with an array of challenges.

According to Meld. St. 9 (2024–2025), and in line with this report, the term 'composite threats' concerns the activities of foreign states which, by their intent, directly or indirectly affect Norwegian security below the threshold of armed conflict. The phenomenon is internationally referred to as, among other things, 'hybrid threats/hybrid conflict' or 'political warfare', and may be confused with 'hybrid warfare' as a military strategy. In this report, the term 'composite threats' is used as defined in Meld. St. 10 (2021–2022) *Prioritized changes, status and measures in the defence sector,* cf. Innst. 392 S (2021–2022), and Meld. St. 9 (2022–2023) *National control and digital resilience,* cf. Innst. 247 S (2022–2023), as well as 'composite use of instruments/composite instruments' as a designation for broad use of instruments.

This means that disinformation is here understood as one aspect of a composite threat (*sammensatt virkemiddelbruk*). This is understood to also be in line with the definition in the *Norwegian Ministry of Defence's long-term plan for the defence sector* (Prop. 14 S (2020–2021)). There, disinformation is described in the following terms:

> The instruments used to achieve political objectives may be diplomatic, informational, military, economic, intelligence-related, and legal. Disinformation, subversion, military signalling, acquisition of strategic resources, control over energy resources, and challenges to our legal order are examples of various forms of instrument use that may represent such threats. The threat of military force creates room for the use of other instruments and can contribute to making these more effective. *(Prop. 14 S (2020–2021), p. 21) (Authors' own translation)*

In the following, we will further define some key concepts for the purpose of this report:

- **Resilience**
- **'Fake news'**
- **Disinformation**
- **Misinformation**
- **Malinformation**

We will also provide a brief definition of **psychological defence**. The purpose of such a clarification on concepts relates to what Caspari (2021) describes as the importance for the national authorities of establishing a common understanding of the given problem in order to meet a hybrid threat. For many countries, including Norway and Sweden, mis-, dis- and mal-information lack a legal or institutional basis and should be considered descriptors of a type of content for an analytical purpose (Pamment & Isaksson, 2024: 7). Generally, what is at stake here is known by

many names, each with at least as many definitions. Also, studies from different disciplines tend to use different concepts to describe similar phenomena, making it challenging to, for example, compare findings across sectors, disciplines and borders (Broda & Strömbäck, 2024). Central to the definition of disinformation, regardless of the exact wording, is the question of *intent*. The intent behind the propagation of disinformation distinguishes it from other forms of incorrect information, and in the following we will briefly describe common definitions of some of these other terms, especially focusing on how they can be distinguished from the term most relevant to this report, *disinformation*.

## 3.1. Defining the concepts

### 3.1.1. Resilience

There are a myriad of different definitions of resilience, emerging across fields, sectors and disciplines. Various definitions exist for resilience with regards to individuals, technology, organizations and authorities, as well as the state and state institutions. In policy and defence contexts, such as in NATO or EU frameworks, societal resilience is often described in more specific and operational terms. For NATO, the common definition is '[t]he ability of a society to resist and recover easily and quickly from such shocks as natural disasters, economic disruption or armed attack' (NATO, 2016). The principle of resilience is rooted in Article 3 of the North Atlantic Treaty: 'In order more effectively to achieve the objectives of this Treaty, the Parties, separately and jointly, by means of continuous and effective self-help and mutual aid, will maintain and develop their individual and collective capacity to resist armed attack.' At the 2016 Warsaw Summit, Allied Leaders agreed to boost NATO's resilience to the full spectrum of threats and further develop their countries' individual capacity in conjunction with NATO's collective capacities to resist any form of armed attack.

They agreed on the following seven baseline requirements for national resilience, against which Allies can measure their level of preparedness:

1. **Assured continuity of government** and critical government services: for instance, the ability to make decisions and communicate with citizens in a crisis.
2. **Resilient energy supplies**: ensuring a continued supply of energy and having back-up plans to manage disruptions.
3. **Ability to deal effectively with the uncontrolled movement of people** and to de-conflict these movements from NATO's military deployments.
4. **Resilient food and water resources**: ensuring resilient supplies that are safe from disruption or sabotage.

5. **Ability to deal with mass casualties and disruptive health crises**: ensuring that civilian health systems can cope and that sufficient medical supplies are stocked and secure.
6. **Resilient civil communications systems**: ensuring that telecommunications and cyber networks can function even under crisis conditions, with sufficient back-up capacity. This also includes the need for reliable communications systems including 5G, robust options to restore these systems, priority access to national authorities in times of crisis, and the thorough assessments of all risks to communications systems.
7. **Resilient transport systems**: ensuring that NATO forces can move across Alliance territory rapidly and that civilian services can rely on transportation networks, even in a crisis.

These baseline requirements do not describe well the individual resilience of citizens, or even of society, understood as made up of individuals. In comparison, the EU uses a definition of resilience that describes it as '[t]he capacity to prepare for, respond to and recover from crises while maintaining the core functions of society' (European Commission, 2020). The EU definition does not necessitate an external 'shock', like the NATO definition can be understood, and this broader view includes elements like public trust, information integrity, civil preparedness and institutional robustness.

This report adopts the following definition:

**Resilience** refers to the capacity of individuals, communities or systems to absorb disturbance, adapt to changing conditions and recover or transform in the face of adversity.[3]

This definition emphasizes three core elements:

- **Absorption**, meaning the ability to withstand shocks and disturbance without collapsing.
- **Adaptation**, the capacity to adjust and continue functioning under new conditions.
- **Transformation or recovery**, meaning the ability to return to a prior state or evolve into a more robust state after a crisis.

In the context of this report, the above definition, and its three crucial elements, implies a focus on individual and systemic flexibility, a changing world and robustness. It also implies that the threats or risks that we need to increase resilience to are not necessarily 'shocks' or 'crises', but rather long-term disturbances and changing conditions, which disinformation is understood to be part of. In the face of disinformation as an element of a hybrid threat, strategically deployed to exploit vulnerabilities, sow confusion and erode trust, we see that efforts to strengthen resilience, in this meaning of the term, become critical. By implicitly taking as a starting point the

concepts of **absorption**, **adaptation**, and **transformation**, this report underscores the importance of both individual and systemic capacities to withstand cognitive and informational threats, adjust to evolving threat landscapes, and emerge stronger. Resilience in this context is therefore not just about preserving the status quo but about developing robust democratic institutions and increasing public awareness.

### 3.1.2. Psychological defence

This report operates with the following definition:

> **Psychological defence** refers to the strategies, capabilities and societal resilience measures designed to protect populations against foreign influence operations and hybrid threats, including disinformation, propaganda and cognitive manipulation.

This is a rather broad definition, derived from the Lund University Psychological Defence Research Institute (Palmertz et al., 2024). It involves public media literacy initiatives, promoting trust in credible information sources and institutions, and building cognitive resistance to influence campaigns. The ultimate goal is to preserve the psychological integrity and democratic functioning of society in the face of deliberate attacks on public perceptions and cohesion.

Against this backdrop, the report now turns to defining several other key concepts, not in terms of the desired outcome (enhanced resilience), but in relation to the challenges that must be addressed: misinformation, malinformation, 'fake news' and disinformation. These terms represent the diverse and evolving landscape of information threats that resilience efforts must be equipped to confront. The following overview starts from the recognition that these terms are often used interchangeably or overlap. However, we would like to point out what we see as differences and nuances, to clarify what we mean by the central concept to this report, namely disinformation. As with resilience, definitions and understandings of these concepts are many and varied. As such, the following short descriptions are not considered to be universally correct; rather, they are acknowledged in the sense that they are widely used.

### 3.1.3. Misinformation

> **Misinformation** can be described as false or inaccurate information shared without the intent to deceive.

In contrast to disinformation, which necessitates intent, scholars like Dame Adjin-Tettey (2022) emphasize that misinformation is disseminated without manipulative or malicious intent.

Misinformation can occur when individuals or organizations unwittingly get the facts wrong. Misinformation often surfaces when a breaking news story is unfolding and details have not yet been confirmed. Another instance of misinformation is when people share false information as a fact without thoroughly checking that the information they are sharing is accurate (Palfrey, 2025).

Example: *Claiming that COVID-19 vaccines contained microchips which were used to track people.*

While this claim is false and has no basis in scientific or technological fact, it was widely circulated online during the pandemic but stemmed from a misunderstanding or misrepresentation of unrelated technology research (e.g., digital vaccine records or injectable tracking devices used in livestock). The reason this is labelled misinformation (and not disinformation) according to Table 1 is that it was shared by individuals who genuinely believed it to be true, without malicious intent. Still, it created harm, but the harm was unintentional. Importantly, however, the impact – that people became more sceptical towards vaccines – was real.

### 3.1.4. Malinformation

**Malinformation** is often described as genuine information shared with the intent to cause harm, often by taking it out of context.

Wardle and Derakhshan (2018) define it as 'information, that is based on reality, but used to inflict harm on a person, organisation or country' (Wardle & Derakhshan, 2018: 44).

Example: *Framing the true claim that a Norwegian military officer was disciplined for misconduct during an overseas deployment as indicative of wider dysfunction within the Norwegian military.*

To label this as malinformation could imply that a foreign-aligned website publishes the real story of the disciplinary case but falsely frames it as evidence of widespread corruption and moral decay within the Norwegian Armed Forces. For example, the article may exaggerate the issue and connect it to NATO cooperation, implying Norway is unfit to lead or host operations. In this case, the claim or statement is labelled malinformation because the core facts of the story are true, but the information is used selectively, out of context, or manipulatively to damage trust in institutions. Here, the intent is to create harm by using reality to undermine credibility, fuel distrust, etc.

### 3.1.5. 'Fake news'

**'Fake news'** implies information presented in the news format and is more commonly used in public debate than scientific research, often to generate clicks or financial gain, or used with political motives.

Example: *A headline in an online newspaper stating: 'Pope Endorses a US Presidential Candidate!'*

In spring 2025, an article falsely claimed that Pope Francis had officially endorsed a specific candidate in the US presidential election. The Vatican publicly denied the claim, and no such endorsement occurred. The article originated from a known website that publishes deliberately fabricated stories to attract clicks and ad revenue. The reason this is labelled as 'fake news' is that it presents itself as a legitimate news article, but the content is entirely fictional. In addition, it is designed to mislead readers and often plays on emotionally charged topics, and it typically circulates rapidly on social media before being debunked. In academia, there is a growing tendency to avoid the term 'fake news', as it is considered as problematic, for example because it can be seen to legitimize anti-democratic propaganda, or because the term has no fixed meaning or fixed function (see e.g., Habgood-Coote, 2018; Coady, 2021).

*In academia, there is a growing tendency to avoid the term 'fake news', as it is considered as problematic.*

### 3.1.6. Disinformation

The key term for this report, **disinformation** is here defined as false information that is deliberately propagated with an *intention to deceive* (see e.g. Aïmeur et al., 2023; Guess & Lyons, 2020; Tandoc, Lim & Ling, 2020) or with an *intention to cause harm* (see e.g. Kapantai et al., 2021).

This means that for something to count as disinformation, three elements should be present:

- The information must be **factually wrong**.
- It must be shared with **intent to deceive, mislead or harm**.
- It must have the **potential to do harm**.

Related to the final element, some refer to the 'Santa Claus test': when we tell our kids that Santa Claus exists, we share factually wrong information with the intent to deceive, but it is difficult to argue that this has the potential to do harm.

> *[Disinformation is] false information that is deliberately propagated with an intention to deceive […] or with an intention to cause harm.*

Disinformation, understood as being made up of all these three elements, is often used as a tool in hybrid warfare, psychological operations or political interference. A characteristic of disinformation is that it is false but may fall below the threshold of an obvious lie (Allcott & Gentzkow, 2017; Lazer et al., 2018). Disinformation can also be a mix of authentic and false information, or consist of information that is slightly distorted, and it is understood as one aspect of a hybrid threat (*sammensatt virkemiddelbruk*), which is in line with the definition in the Norwegian Ministry of Defence's long-term plan for the defence sector (Prop. 14 S (2020–2021)). At a conceptual level, the intent behind the propagation of disinformation distinguishes it from other forms of false information. According to recent research on the Norwegian secret service's understanding of disinformation as a societal threat, disinformation is the term most widely used within these services (Samuelsen, 2023). In practice, however, labelling social media content or other material as disinformation can be challenging, as it requires intelligence regarding the origin of the content. We will give two fictional examples of disinformation:

Example 1: *Claiming that a fabricated document 'proves' that NATO is planning to invade a neighbouring country and sharing the document online via state-linked social media accounts.*

In this example, the document is fake and is created and distributed intentionally as part of an influence operation. Its goal is to undermine trust in NATO, provoke fear, and justify aggressive actions by the state spreading it. The reason this is labelled as disinformation is that the information is knowingly false and spread deliberately to deceive and manipulate public perception or policy. In this example, as often is the case, the act serves a strategic, often geopolitical purpose, typically linked to state or state-backed actors. This type of threat is much harder to detect and counter because it often blends partial truths, fake documents, or manipulated media, and may exploit existing tensions or narratives.

Example 2: *A hostile state actor launches a campaign (e.g. through proxies or fake accounts) claiming: 'NATO is secretly planning to establish permanent military bases in northern Norway in violation of Norwegian policy.'*

Here, the intent is to undermine public trust in Norway's defence policy and stir anti-NATO sentiments. This can be achieved through tactics such as fake expert quotes, forged documents, 'leaked' reports, etc., shared through channels such as anonymous social media accounts or state-aligned media.

The present report adopts the concept of disinformation as its analytical starting point, and although not universally adopted as the true definitions, we thus find it useful to provide the following overview in Table 1 as the basis for the remainder of the report.

> *[F]or something to count as disinformation, three elements should be present: the information must be factually wrong; it must be shared with intent to deceive, mislead or harm; and it must have the potential to do harm.*

| Term | Truthfulness | Intent to Deceive | Reason for sharing |
|---|---|---|---|
| **Misinformation** | False | No | Often accidental |
| **Disinformation** | False | Yes | To deceive in order to manipulate |
| **'Fake news'** | False/fabricated | Yes | To generate clicks to serve a political agenda |
| **Malinformation** | True (but harmfully decontextualized) | Yes | To harm, blackmail or sabotage |

Table 1: Attributes of relevant concepts

## 3.2. Acknowledging contestations

As mentioned, there seems to be an emerging tendency among scholars to avoid the use of 'fake news', for example because of its current political connotations. Efforts to distinguish it clearly from disinformation indeed seem relevant both in principle and practice. In a report by Pammant and Isaksson (2024) from Lund University Psychological Defence Research Institute, one of the points of concern for the Swedish Agency for Psychological Defence (MPF) is precisely a lack of conceptual clarity over the nature of the challenges faced by governments in this area. Pammant and Isaksson refer to the fact that while popular culture characterizes the new media landscape as corrupted by 'fake news', the emerging international policy area was initially characterized by the term disinformation. They write that 'over time it has become clear that use of the term disinformation as a catch-all is both problematic and misleading' (Pammant & Isaksson, 2024: 23). The establishment of psychological defence as an alternative conceptualization for the policy area in the Swedish context is therefore, as described by the MPF, a significant development of the policy area, with potential consequences for international partners (Pammant & Isaksson, 2024: 23).

In the conceptualization in the report from Lund University Psychological Defence Research Institute (2024), the use of the term disinformation serves as shorthand for three overlapping groups of problems:[4]

1. The first group of problems is the **spread of false information**, whether deliberately or inadvertently, by individuals communicating through traditional and social media. Debates in this area are fundamentally about the quality of deliberation in the public sphere, as well as protection of fundamental freedoms such as expression.
2. The second group of problems is the more complex phenomena of **influence campaigns** driven by motivated organizations capable of coordination, using multiple communication tools, and conducting clandestine activities. Such coordinated activities are often referred to as 'operations' or 'campaigns' to emphasize the complex and opaque nature of the planned influence effort.
3. The third group of problems is **foreign interference**, which takes place in the context of other hybrid, cyber and espionage activities that hostile states conduct. It positions influence campaigns within the broader bilateral relationship with a hostile foreign power.

In the view of the MPF, these groups of problems overlap, but are distinct to the degree that different actors are involved in monitoring, educating and responding to the threats.

The focus on concepts and definitions is not merely about semantics. As Ibrahim, Rhode and Daseking (2023) note in their systematic review of cognitive and psychological warfare, the lack of terminological clarity in this domain can hinder effective governance and international cooperation. As was also highlighted by the leader of the research group on 'Cognitive Warfare' in the CENTREPEACE project, Petra Mljenková from Masaryk University in the Czech Republic, the operational consequences of using conceptually fragmented frameworks and terms are that it can lead to incompatible threat assessments, coordination gaps and unaligned policy responses. This was underlined during an international workshop in Helsinki in May 2025, where the topic was 'Conceptualising Cognitive Warfare'. Also in this context, the fact that definitions indicate responsibility was highlighted, and a take-away from the workshop was that there is an urgent need for improving cooperation in the field. While different conceptualizations were presented and discussed, a key insight remains that there is indeed no commonly accepted definition of either disinformation or related concepts, but that there is value in itself in discussing them.

Disinformation is only once piece of the puzzle, the definition of which also varies. As already mentioned, in this report disinformation is understood as one aspect of a hybrid threat (*sammensatt virkemiddelbruk*), which is in line with the definition in the Norwegian Ministry of Defence's long-term plan for the defence sector (Prop. 14 S (2020–2021)). Increasingly, actors such as NATO have begun to frame disinformation and related challenges within the concept of cognitive warfare, which explicitly targets the human mind, our perceptions, beliefs, and decision-making processes, as a domain of conflict (NATO, 2021). Some experts, like Le Guyader (2022), argue that the cognitive domain should be formally recognized alongside land, air, maritime, space and cyberspace as a distinct operational environment. This shift reflects a growing awareness

that influence operations are not merely about spreading falsehoods, but about shaping societal narratives, exploiting divisions and undermining trust. This is also why countering the spread and existence of disinformation is something distinct from countering its negative effects on the public. However, according to Wigell (2021), there is also a link between the two. Wigell emphasizes that efforts focusing on strengthening democratic norms and values can in theory be strategic instruments used also to deter authoritarian regimes. The term 'democratic deterrence', in contrast to traditional deterrence theory, is based on society's collective resources, the use of soft power and non-military means to achieve limited deterrence (Wigell, 2021). In this sense, resilience building can theoretically also contribute to a form of 'democratic deterrence', although we do not assume that implementing measures along the lines of psychological defence will automatically deter foreign states from malign intervention (such as influence operations). We do, however, see them as contributions to building societal resilience.

*Increasingly, actors such as NATO have begun to frame disinformation and related challenges within the concept of cognitive warfare.*

The concept of cognitive warfare developed under NATO's Allied Command Transformation (ACT) provides a starting point for the broader conversation around cognitive threats. It explores how adversaries exploit human cognition to manipulate perceptions, disrupt decision-making and influence behaviour. Recently, the term 'cognitive security' has also emerged as a concept that '(...) blends insights from diverse disciplines and focuses on the intersection of technology and social engineering in hybrid campaigns. While cognitive warfare is an emerging military concept focused on hostile tactics, yet to be formalized into a doctrine or domain, the concept of cognitive security extends this logic into a broader defensive framework' (Catena et al., 2025). For example, Grahn & Taipalus (2025) suggest the concept of 'cognitive security' aimed at merging common academic definitions with the use by the NATO/EU. Cognitive security can here be defined as a state and a process in which malign influence or manipulation cannot affect human cognition, achieved through a combination of knowledge, situational awareness and purposeful actions (Grahn & Taipalus, 2025). To achieve cognitive security, they point to several factors from the literature which enhance this state, such as: situational awareness; pre-bunking (a proactive strategy that prepares people to recognize and resist misinformation before it spreads) and information inoculations; digital literacy, media literacy and information literacy; critical thinking; reducing cognitive biases; emotional regulation and metacognitive skills. Specifically, the factors of knowledge and situational awareness are highlighted as especially critical.

The acronym FIMI (Foreign Information Manipulation and Interference) has recently met a lot of success and has become widespread in the European Union, within the European External Action Service (EEAS) and across the Member States. Therefore, it deserves to be well understood and carefully defined. In fact, FIMI overlaps to a considerable extent with disinformation, but some nuances need to be highlighted: not all disinformation is FIMI, and FIMI is not only

disinformation. I.e. FIMI can be described as foreign-run, coordinated manipulation operations that may use disinformation as one tool. Eventually, the phenomenon pushes us to consider state-sponsored manipulations of information in a new light, at the crossroads of influence operations and cyber-security, to better develop effective countermeasures (EU Disinfo Lab, 2023). Furthermore, according to RAND Corporation, 'Information operations and warfare', also known as influence operations, include the collection of tactical information about an adversary as well as the dissemination of propaganda in pursuit of competitive advantages over an opponent. Relatedly, they define psychological warfare as involving the planned use of propaganda and other psychological operations to influence the opinions, emotions, attitudes and behaviour of opposition groups (RAND, 2025). Disinformation can be one element of both influence operations and psychological warfare, but we find that there are reasons to be careful not to use the terms interchangeably.

In addition to the value of conceptual clarity, using the term 'war' in contexts such as 'psychological warfare' or 'information warfare' carries implications that go beyond semantics. One of the primary issues is the militarization of language. Referring to disinformation, or the information operations in which it plays a part, as a form of warfare can be said to impose a military framing on what might rather be political, social or informational challenges. In theory, this framing may escalate tensions, justify exceptional measures like surveillance or censorship, and contribute to a blurring of the boundaries between civilian and military domains.

Conceptually, some also point to the potential that the use of 'war' risks inflating the perceived threat and oversimplifying complex phenomena. Disinformation, for instance, is not always the product of coordinated, hostile intent, but it can also be decentralized and non-state driven. Not all influence is adversarial, and some is part of legitimate political discourse. Framing such activities as warfare may obscure these nuances. According also to Hayward (2025), the term disinformation is generally used to refer to information that is false and harmful, in contrast to misinformation (false but harmless) and malinformation (harmful but true); disinformation is also generally understood to involve coordination and to be intentionally false and/or harmful. However, Hayward (2025) also notes that particular studies rarely apply all these criteria when discussing cases, and that doing so would involve applying at least three distinct problem framings:

> […] an epistemic framing to detect that a proposition in circulation is false, a behavioural framing to detect the coordinated efforts at communicating that proposition, and a security framing to identify threats or risks of harm attendant on widespread belief in the proposition. As for the question of intentionality, different kinds of clues can be picked up within each framing, although none alone is likely to be conclusive. Yet particular studies tend to centre on or prioritise a single framing. Many today aim to make policy recommendations about combatting disinformation, and they prioritise security concerns over the demands of epistemic diligence. This carries a real risk of disinformation research being 'weaponised' against inconvenient truths. *(Hayward, 2025: 1)*

The problem with this, according to Hayward (2025), is that not recognizing the importance of what he calls 'epistemic diligence' (checking the veracity of the claim) and transparency about normative assumptions can lead to confusion and intractable difficulties in reaching shared understandings of what is at stake in a given situation. Furthermore, strategic framing also affects public perception. Describing influence operations as a form of war may contribute to a heightened sense of threat among the public and policymakers, potentially encouraging more defensive or assertive policy responses. If we follow this rationale, we can say that it may also theoretically contribute to a polarization of public opinion and reduce the space for democratic deliberation and nuanced debate.

> *Referring to disinformation […] as a form of warfare can be said to impose a military framing on what might rather be political, social or informational challenges. In theory, this framing may escalate tensions, justify exceptional measures like surveillance or censorship, and contribute to a blurring of the boundaries between civilian and military domains.*

In sum, the aim of the above description of some challenges and contestations when it comes to the words used to describe disinformation and related phenomena has been two-fold: to underline the importance of concept clarification in general, and specifically to highlight some potential pitfalls when using certain terminology. In the next part of the report, we will look at different ways in which resilience can contribute to countering the negative impacts of disinformation. First, we describe the link between defence against disinformation and resilience, before listing some key initiatives for strengthening Norwegian defence and societal resilience to disinformation, focusing on the main strategic and policy processes. We then briefly deliberate on increasing resilience to disinformation in peacetime versus war, drawing on insights from Ukraine, France and Finland.

# 4. Resilience against disinformation: Norwegian and European approaches and procedures

As defined in Chapter 3, understanding resilience as 'the capacity of individuals, communities or systems to absorb disturbance, adapt to changing conditions and recover or transform in the face of adversity' in this context means that we focus on three core elements: the ability for Norwegian society to *withstand* disturbance (i.e. disinformation) without collapsing; the capacity of Norwegian society to *adjust* and continue functioning under new conditions; and the ability for Norway to *evolve* into a more robust actor as a result of the disturbance (e.g. enforcing trust and other democratic values).

Resilience to disinformation, and (psychological) defence against it, are two closely connected issues. On the one hand, we see resilience as a foundation or precondition for defence. This means that resilience provides the underlying capacity of a society to withstand, adapt to and evolve from the negative effects of disinformation. It also means that we see resilience as a proactive condition that enables societies precisely to absorb the impact of disinformation, adapt to evolving conditions, and transform in ways that strengthen democratic institutions and public trust. In this sense, resilience is not separate from defence, but rather a core component of it. In addition, the two concepts are interlinked in the way that we see (psychological) defence against disinformation as one way to build resilience. This means that the various efforts to counter disinformation (e.g. awareness-raising) are understood as defensive strategies that contribute to building or operationalizing resilience.

In sum, we can say that there is a mutual reinforcement when we consider the relation between resilience to disinformation and the (psychological) defence against it, where resilient societies are better equipped to defend themselves against disinformation, and effective defence strategies or efforts further enhance societal resilience. To address this dynamic of mutual reinforcement, we loosely draw on the framework proposed by Kalenský et al. (2022), which identifies four lines of defence against disinformation, with two considered relevant here:

1. **Detection, monitoring and documentation**
   This first line of defence focuses on achieving situational awareness through comprehensive data collection. It involves identifying and tracking disinformation campaigns, analysing their messages and narratives, and mapping the channels through which they are disseminated. As the topic of this report concerns raising societal resilience, we consider efforts in this line to fall outside the scope of this report.
2. **Raising awareness**
   The second line aims to inform and prepare the public. By disseminating insights from the first line, this approach seeks to warn audiences about the nature, goals and effects of disinformation campaigns, thereby building societal resilience against manipulation.

3. **Repairing and preventing systemic weaknesses**
   This line targets vulnerabilities within the information ecosystem that disinformation actors exploit. Key areas include low media literacy, diminished trust in institutions, the influence of social media platforms, and the weakened role of traditional media and civil society.

4. **Limiting and sanctioning perpetrators**
   Unlike the previous lines, which focus on strengthening the resilience of targets, the fourth line addresses the aggressors. Efforts in this line also fall outside the scope of this report.[5]

Lines 2 (raise awareness) and 3 (target vulnerabilities), thus provide a starting point for the next chapters. Raising awareness, according to Kalenský et al. (2022), implies focusing on disinformation campaigns, warning the public about the messages, narratives, goals, channels and effects of these campaigns, and thus inoculating the public against disinformation. Here, the emphasis shifts to disseminating information to the public as preparation for the threat. Targeting vulnerabilities implies countermeasures focusing on repairing and preventing some of the 'systematic weaknesses within the information ecosystem that the disinformation actors exploit' (Kalenský et al., 2022). These could be low levels of media literacy, general lack of trust in institutions and specifically in their capabilities to counter disinformation, the social media environment, and the weakened position of the traditional media or civil society.

## 4.1. Approaches to strengthening resilience to disinformation in Norway

Implicitly acknowledging the importance of both awareness-raising and targeting vulnerabilities, over the past decades, Norway has recognized that national security is not solely a matter of military strength, but also of societal cohesion, institutional trust, and the ability to withstand complex and evolving threats. From early post-war reflections on psychological defence to recent strategies addressing disinformation and hybrid threats, the Norwegian approach has increasingly emphasized resilience as a whole-of-society responsibility. This evolving understanding has been shaped by a series of commissions, white papers and strategic frameworks that reflect both historical continuity and an adaptation to new geopolitical and technological realities. The threat which disinformation represents is one aspect of this new reality. The following overview highlights key milestones in efforts to build resilience.

The Defence Commission of 1946 highlighted psychological defence as an important part of Norway's overall defence. In its main recommendation for a Norwegian defence organization, it was emphasized that defence, in addition to the military component, must also include civil, socio-economic and psychological defence. This illustrates that the idea of resilience against various types of threats, also below the threshold of war, has long been considered essential in Norway

(Gjeseth, 2016). In recent years, Norway has taken several important steps to increase national resilience to disinformation and related threats; in the following, we will briefly address the most important.

- In 2020, the Norwegian government presented **Prop. 14 S (2020–2021), the Long-Term Plan for the Defence Sector**, which laid out strategic priorities for the coming years. The document reflected a broader understanding of modern threats that go beyond conventional military challenges. The use of the concept 'composite use of means' (*sammensatt virkemiddelbruk*) acknowledges that adversaries increasingly employ a mix of different tools – including cyber operations, economic pressure and disinformation – to influence and destabilize democratic societies.
- **In 2022, the Commission on Freedom of Expression delivered its report, NOU 2022:9**, which undertook a comprehensive assessment of the state of free speech in Norway. The commission examined how digital transformation, social media platforms and emerging information threats – particularly disinformation and polarization – are affecting public discourse and democratic engagement. Among its recommendations were measures to strengthen media literacy, support independent journalism, and ensure that digital platforms operate in ways that promote transparency and accountability. Importantly, the commission's work contributed to a broader understanding of how information integrity and psychological resilience are essential components of national preparedness. It reinforced the idea that defending democratic values requires not only legal protections for speech, but also proactive efforts to cultivate a healthy and inclusive information environment.
- **The Total Defence Commission of 2021** delivered its report in May 2023. The report, **NOU 2023:14** *Forsvar for fred og frihet* (*Defence of peace and freedom*), evaluated Norway's 'total defence' concept, emphasizing civil-military integration and preparedness across sectors. The report contributed to broader discussions on hybrid threats, societal resilience and cross-sector coordination. The Commission underlined the need to raise public awareness about the threat and risk landscape, as well as measures to reduce societal vulnerabilities. Although the organization of 'a modern psychological defence' is not described in NOU 2023:14, the Commission describes how the high level of trust that characterizes Norwegian society is the key foundation for the population's ability to resist disinformation, attempts at division, and exploitation by foreign actors (NOU 2023:14: 224).
- **The Total Preparedness Commission of 2022** was appointed by Royal Decree on 21 January 2022 to assess how Norway's overall preparedness resources can be utilized most effectively. The Commission's mandate encompassed the entire spectrum of crises. Its discussion of the comprehensive risk, vulnerability and threat landscape was based on four broad factors affecting Norway: great power rivalry, technological development, climate change, and demographic shifts. In its report, **NOU 2023:17** *Nå er det alvor: Rustet for en*

*usikker fremtid* (*Now it's serious: Prepared for an uncertain future*), the Commission points out that several countries have in recent years intensified their efforts to combat hybrid threats, hereunder disinformation. The Commission recommended establishing a Norwegian national body for monitoring and analysing attempts at influence operations, separate from the intelligence and security services.

- Based on NOU 2023: 17, the government delivered the **Meld. St. 9 (2024–2025): White Paper on Total Preparedness**, which presented the role and framework conditions for editor-controlled media, the population's critical media understanding, and for monitoring the influence of major technology platforms on public discourse. It also summarized existing knowledge about and research on the spread of disinformation and its consequences for Norwegian society (Meld. St.9 2024–2025: 98f). The white paper states the role of the MoD in this regard:

  > The Ministry of Defence is responsible for influence operations aimed at the defence sector, defence policy and defence capability or which may otherwise constitute a military threat to national security, as well as international defence cooperation in this area. *(St. Meld 2024–2025: 99)*

  The white paper includes over 100 actions to strengthen civil preparedness, leadership and resilience against hybrid threats, and the government formulated seven strategic points for future development of national preparedness; one of these points is to increase public resilience, in order to preserve high societal trust. Although the government, according to the white paper, did not consider it appropriate to create a new agency as a centralized hub for countering disinformation, it recognizes the need for a more integrated and comprehensive approach to handling disinformation and other information threats.

- In June 2025, a **National Strategy for Strengthening Resilience to Disinformation (2025–2030)** was launched. The strategy highlights, among other things, that geopolitical tensions, increased polarization, and war in Europe have further heightened interest in the spread of misinformation and disinformation. Furthermore, technological developments have made it easier to both produce and disseminate disinformation quickly and at low cost. The strategy includes over 40 measures built around five main focus areas:

  1. **Strengthening critical media literacy in the population.** The government will consider establishing a new centre for source awareness, enhancing libraries' work on digital inclusion, and supporting initiatives to increase resilience to disinformation through EEA grants.

  2. **Holding social media platforms accountable.** The government will ensure the swift implementation and effective enforcement of new EU regulations such as the Digital Services Act (DSA), the AI Act, and the Media Freedom Act. These aim to increase transparency around algorithms, improve protection for children and youth,

strengthen press freedom on digital platforms, and enable enforcement of accountability measures for large digital platforms. The government will prioritize documenting violations of these regulations.

3. **Strengthening editor-controlled media and journalism.** The government emphasizes the importance of editor-controlled media for a resilient society and will, in light of this, review media support schemes in the upcoming four-year policy cycles. It will also consider new measures to encourage more young people to engage with editor-controlled media, support investigative journalism, and contribute to skills development in newsrooms.

4. **Enhancing knowledge and research.** The government will assess the establishment of a new research centre to monitor developments in public discourse, including disinformation and polarization. Although Norwegian society has so far proven resilient, there is a need for long-term research to track developments over time.

5. **Strengthening government efforts and coordination.** The government will expand the mandate of the Norwegian Media Authority to strengthen resilience to disinformation. The Authority will, among other things, contribute to analyses of how social media algorithms affect the spread of editorial content on one hand and disinformation on the other. Furthermore, the government will work broadly to ensure more holistic prevention and management of influence attempts.

- The first **National Security Strategy** was launched by the Prime Minister's Office in September 2025. The strategy identifies three main strategic priorities in response to the current challenges.

  1. **To rapidly strengthen Norwegian defence capability.** This means to be prepared for the fact that war could once again come to Norway. Within the framework of NATO, it underlines that work must be done to ensure that Europe assumes far greater responsibility for its own security.

  2. **To increase the resilience of Norwegian society.** This means to ensure a common understanding of current threats and working together to reduce vulnerabilities and strengthen the ability to deal with serious incidents.

  3. **To strengthen economic security.** To do so, the strategy states that the competitiveness of the Norwegian economy must increase, and to reduce vulnerabilities vis-à-vis countries with which Norway has no security cooperation and strengthen the economic cooperation with allies and partners.

  Delivering on these priorities will require a whole-of-society approach, from the central government to private companies, trade unions, the voluntary sector, municipalities and ultimately every Norwegian citizen.

Especially since 2018, there has been a **strong emphasis on self-preparedness** by the Norwegian Directorate for Civil Protection (DSB). As the overview above illustrates, Norway has long sought to strengthen its preparedness and protect democratic values in the face of emerging influence operations and information threats. However, in 2026 perhaps more than ever before, a comprehensive strengthening of national preparedness is seen as a collective effort which requires the participation of the entire population. According to the DSB, on an individual level, high personal preparedness creates a resilient population, which is fundamental to a strong total defence. Thus, in autumn 2018, the campaign 'You are part of Norway's preparedness' was launched. The main message was that everyone should consider what kinds of incidents and accidents might occur, and plan to be able to take care of themselves and those around them for at least three days in the event of a failure of critical infrastructure, such as electricity, water or mobile networks. The advice has been updated several times, and in 2024, 'critical source awareness' was for the first time defined as part of one's personal preparedness (Aarli-Grøndalen, 2024). As part of the so-called 'Personal preparedness week', the DSB distributed a new physical version of the campaign brochure to all Norwegian households with advice on personal preparedness. Importantly, for the first time, the brochure includes guidance on source criticism. The Norwegian Media Authority stresses that these recommendations are especially important in the event of a crisis, but that they should also be followed in everyday life. The baseline for these campaigns is that each one of us has a responsibility to follow the self-preparedness advice and prepare for situations where normal societal functions are lacking.

Although preparedness as a way of building resilience against disinformation is partly an individual responsibility, facilitating coordination between the different actors in this field on a national level happens in various ways. 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 the 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. These work together to strengthen the national capability to identify, build understanding of, and provide decision-making support related to hybrid threats including Information Influence Operations (IIOs). Internationally, Norway participates in several networks to strengthen national capacities to respond to IIOs, primarily to share and receive information on current events, trends and countermeasures. These networks include the NATO RRG (Rapid Response Group) 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 2025–2026 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.[6]

As we see, efforts to counter, and limit the adverse effects of, disinformation in Norway are increasingly focused on improving coordination across sectors and levels of governance. A recent key development in this regard is the government's efforts towards establishing a National Centre for Source Awareness as part of its new strategy for strengthening societal resilience against disinformation (2025–2030). On 15 October 2025, the Norwegian government announced its support for the initiative by allocating NOK 20 million for the establishment of the *Tenk – Senter for kildebevissthet* (*Think – Center for Source Awareness*), an initiative led by Faktisk.no. The centre would be established as a foundation with NTNU, the Norwegian Children and Youth Council (LNU), the Norwegian Publishers Association, and the Norwegian Press Association as founders. The centre would build on the work already being done by the current school division of Faktisk AS. The school division of Faktisk, which is called Tenk, would become part of the new centre. This funding is part of a broader increase of NOK 23.5 million for media-related measures aimed at implementing the national strategy against disinformation.

## 4.2. Approaches to strengthening resilience to disinformation in the EU

Efforts to counter disinformation, and to increase resilience to it, have been long ongoing, in Europe and elsewhere. At the European level, the EU launched its main counter-disinformation initiative a little over ten years ago, in 2015, with the *EUvsDisinfo* campaign. Later, incidents like Russian interference in the 2016 US elections triggered an EU response particularly focused on countering disinformation on social media. In 2018, the European Commission presented an action plan to the European Parliament and the European Council on how to combat disinformation in the lead-up to the EU elections of 2019, the goal being to 'protect the Union's democratic systems and combat disinformation, including in the context of the upcoming European elections' (European Commission, 2018). The action plan consisted of four pillars:

i. Improving the capabilities of Union institutions to detect, analyse and expose disinformation.
ii. Strengthening coordinated and joint responses to disinformation.
iii. Mobilizing the private sector to tackle disinformation.
iv. Raising awareness and improving societal resilience.

One of the concrete measures to come out of this action plan is the *Rapid Alert System* (RAS), which is intended to 'facilitate the sharing of insights related to disinformation campaigns and coordinate responses' (RAS Factsheet, 2019).

In 2018 the EU also released a *Code of Practice on Disinformation*, which was further strengthened in June 2022 in the wake of both the full-scale invasion of Ukraine and the COVID-19 pandemic. The widely disseminated disinformation campaigns around COVID-19 led to a growth in countermeasures, which resulted in the introduction of more elaborate approaches, like the

FIMI toolbox introduced in 2021 (Kalenský & Hanhijärvi, 2025: 5). As described by the European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE), other countries, such as the UK, have produced their own toolkits for countering disinformation, and others still went as far as introducing new institutions dedicated to countering disinformation, information manipulation, or related problems (Kalenský & Hanhijärvi, 2025: 5). A recent report from the Hybrid CoE shows that while there are many good measures to counter disinformation in place across the Euro-Atlantic region, practitioners in EU and NATO countries largely state that all lines of their counter-disinformation work are under-resourced (Kalenský & Hanhijärvi, 2025: 4). The report also points to the fact that there seems to be a lack of established mechanisms for cooperation between the authorities and the non-governmental sector – that neither of the two sectors sees the full picture, making it necessary to exchange information regularly (Kalenský & Hanhijärvi, 2025: 4). In Norway, the sectorial principle (*sektorprinsippet*) has traditionally been strong. The principle ensures that the sectors have the necessary freedom to carry out their tasks, and it assigns constitutional responsibility to each individual minister. However, some areas require cross-sectoral governance and joint efforts and cooperation across sectors. We see for example that the Norwegian National Security Agency (NSM) holds a lot of information which could be useful for other sectors.

A basis for this PRIO Paper is that learning from how other countries approach institutional resilience to disinformation can offer valuable insights for Norway. In the following sections, we take a closer look at how a few European countries have organized their efforts in this area. Particular attention is given in Chapter 5 to the Swedish approach and the role of the Swedish Psychological Defence Agency (MPF). This focus is motivated not only by the uniqueness of this recently established agency, but also because it provides some basis for comparison for Norway. Notably, however, the Swedish context is also different. For example, the Swedish agencies and authorities are organized so as to operate more autonomously, as was evident for example during the COVID-19 pandemic. Nonetheless, Sweden's experience provides a useful reference point for understanding how similar states might respond to the challenges. The selection of a few other empirical contexts is based on their prominence in the research literature or policy reports, the fact that they represent known cases of disinformation, or that they include learning points which are deemed relevant to explore here.

The descriptions of other empirical contexts should also be read in relation to other publications and policy reports on this topic, related both to defence and preparedness. For example, the 2022 report by the Norwegian Defence Research Establishment (FFI) to the Defence Commission (*Forsvarskommisjonen*), which conducted a study of how other countries address complex threats. Specifically, FFI was commissioned to consider what Norway can learn from Finland, Sweden, Estonia, the United Kingdom, the Netherlands and Australia regarding how they work to deter, detect and respond to hybrid threats. While the focus in the study by FFI was on state approaches and best practices as per 2022, the current report expands on this not only by taking societal

resilience as a starting point, but also by providing insights into the situation in Sweden in particular, with the MPF having been operating for almost four years now. Additionally, the analytical focus of the current report is not directly related to 'deterring' and 'detecting' hybrid threats, but rather on building societal resilience as a *response* to disinformation. However, best practices identified in the countries included in the 2022 report by FFI also highlight the importance of increased awareness and understanding of threat dynamics, value systems and societal vulnerabilities. This includes clarifying roles and responsibilities among key actors and emphasizing the need for strengthened coordination and collaboration. Here, too, a key focus is resilience. Bergaust et al. (2022) write:

> The largest room for development in Norway as a liberal democracy is to strengthen resilience in our democracy, in critical infrastructure and in the population. The Defence Commission should consider how a modern psychological defence could be organised in Norway.

It is also relevant to stress that efforts to build societal resilience and trust should not be limited to times of crisis or conflict. Strengthening these capacities during periods of stability can help create a more robust foundation for responding to future challenges, while also supporting democratic cohesion and public confidence in institutions.

> *Strengthening societal trust and preparedness during times of stability not only reinforces democratic values but also ensures that Norway is better equipped to respond to future disruptions.*

In the Norwegian setting, where trust in institutions is generally high and society is relatively cohesive, it seems especially important to invest in resilience-building outside of acute crises or conflict. Strengthening societal trust and preparedness during times of stability not only reinforces democratic values but also ensures that Norway is better equipped to respond to future disruptions, whether these arrive in the form of disinformation, hybrid threats, the next pandemic, or other crises.

### 4.2.1. France and Finland

From what we have seen, despite differences in labels, terms and concepts, many countries have measures to protect the civil population or the public via information. The approach to countering disinformation varies across the Nordics and the European Union, and combines regulatory measures, strategic partnerships, and media literacy initiatives. Efforts in place to do this generally also acknowledge the importance of safeguarding core democratic principles, such as the freedom of expression. Key measures by the EU include the previously mentioned *Code of Practice on Disinformation* and the *Digital Services Act* (DSA), which aim to hold digital platforms accountable and ensure transparency. In addition, initiatives such as the East StratCom Task

Force and the Rapid Alert System highlight the European Union's efforts to counter disinformation as a tool of hybrid warfare (D'Andrea et al., 2025).

While such efforts are generally implemented on the structural level, the role of the citizen is also considered of great importance, as the EU approach fundamentally seeks to empower individuals through media literacy programmes intended to enable them to recognize and resist manipulative content. On the European level, media literacy programmes are growing significantly in number as a concrete way of making individuals more resilient. Also in Norway, the establishment of Faktisk.no, as well as several campaigns by The Norwegian Media Authority (*Medietilsynet*), such as 'Stop. Think. Check', has in recent years aimed at increasing media literacy through different forms of fact checking.

Although fact-checking initiatives and media literacy programmes are emerging across Europe, and despite joint initiatives and European regulations such as the DSA, the specific approaches vary in different countries and contexts. Dedicated initiatives exist in for example Finland, Estonia and The Netherlands (Bergaust et al., 2022), ranging from single information campaigns to dedicated national agencies working specifically towards making individuals aware of their potential exposure to influence from foreign powers, and by providing them with tools to detect and manage such influence. In general, to counter malign influence campaigns, a coordinated psychological or cognitive defence effort starts from the acknowledgement that the first line of defence against disinformation consists of source-critical individuals. According to Bergaust et al. (2022), best practice from other countries points to the importance of strengthened awareness and knowledge of three dimensions: threat, value and vulnerability. This includes a clarification of the roles and responsibilities among key players and emphasis on strengthened collaboration.

In France, the government recently established a dedicated agency to combat foreign disinformation and "fake news", Vignium (Service for Vigilance and Protection against Foreign Digital Interference). This was launched in response to rising threats of foreign digital subversion and was a key initiative within France's General Secretariat for Defence and National Security (SGDSN), which operates under the authority of the Prime Minister of France. Established on 13 July 2021, in response to the so-called Macron Leaks – attempts by Russia to interfere in the 2017 French presidential election – the initiative has grown to include approximately 50 employees (Freihse & Bochert, 2024). They come from diverse fields such as Open-Source Intelligence (OSINT), data science, political science/geopolitics and digital marketing. Viginum is supported by a scientific and ethical committee that publishes an annual report evaluating its activities. The agency specializes in monitoring and countering foreign disinformation efforts online, and functions as a rapid-response unit; its analysts conduct open-source investigations, map emerging disinformation tactics, identify the actors behind them and promptly brief political decision-makers (Vignium, 2022). Notably, the agency's nimble analysis-to-denouncement pipeline is considered a key asset in raising public awareness and reinforcing societal resilience.

*[France] recently established a dedicated agency to combat foreign disinformation and 'fake news' […]. The agency specializes in monitoring and countering foreign disinformation efforts online, and functions as a rapid-response unit; its analysts conduct open-source investigations, map emerging disinformation tactics, identify the actors behind them and promptly brief political decision-makers.*

**Finland** has established itself as a global leader in media literacy, consistently topping the Media Literacy Index for seven consecutive years. Its success stems from a comprehensive, education-based approach that begins in primary school, where students learn critical thinking and how to evaluate information. Media literacy is integrated into the national curriculum, ensuring that young citizens develop the skills needed to navigate complex digital environments. This commitment seems especially vital given Finland's geopolitical position bordering Russia. In response to sophisticated disinformation campaigns, Finland has implemented a proactive digital defence strategy. Authorities focus not only on verifying content but also on identifying and disrupting the fake accounts that spread false narratives. Finland's model demonstrates how investing in media literacy can be seen as a strategic tool for democratic resilience. By equipping citizens with the ability to critically assess information, Finland thus strengthens its defences against disinformation and might be seen to offer a blueprint for other nations facing similar threats (DISA Press Room, 2025).

*Media literacy is integrated into the national curriculum [in Finland], ensuring that young citizens develop the skills needed to navigate complex digital environments.*

According to the Total Defence Commission, Norwegian authorities can draw inspiration from Finland, where, as mentioned, psychological resilience is given particular emphasis (Wither, 2020). The Commission specifically underlines that psychological resilience in Finland:

> […] is supported by a range of training and educational programmes within the Finnish security concept. These include national courses at the Finnish Defence University, tabletop exercises for political leadership, cross-sectoral drills and the integration of complex threat scenarios into university curricula. *(NOU 2023:14: 224) (Authors' own translation)*

Further, the Commission states that '[t]raining activities have also been conducted in the private sector, along with initiatives to enhance media literacy among the population' (NOU 2023:14). Ensuring a free, diverse and responsible media has been highlighted as an essential part of the Finnish security concept, and within the Finnish Government's Situation Centre, a group has been established to analyse complex threats, comprising representatives from all ministries, academia and the private sector. In sum, psychological resilience is an integrated part of the Finnish

national security strategy, and the concept seems to be interpreted rather broadly by the Finnish Security Committee (The Security Committee, 2017: 22):

> Psychological resilience means the ability of individuals, communities, society and the nation to withstand the pressures arising from crisis situations and to recover from their impacts. Good psychological resilience facilitates the recovery process. Psychological resilience is expressed in the citizens' will to defend their country's independence as well as in the determination to maintain the livelihood and security of the population in all situations. Creating and maintaining psychological resilience is a longstanding and cross-cutting effort involving different administrative branches.

Here, we also see the expressed link between the will to defend and psychological resilience, and an underlining of the necessity of long-term investments and efforts across sectors.

### 4.2.2. Ukraine

To be able to convey correct and important information to the public during peacetime is one element of both safeguarding the population as well as building resilience to disinformation. However, complexity is added when such information is to be disseminated by the authorities to the public during war. For example, the State Emergency Service of Ukraine (SESU) faces an enormous task in preventing civilians from coming into contact with dangerous mines. As a way of managing the fear of mines in the Ukrainian population, public communication is key. To achieve this, the SESU uses a combination of digital and physical means to inform the civil population of the dangers and whereabouts of mines. This encompasses for example posters in supermarkets, on buses, and train stations.[7]

Ukraine has developed a comprehensive strategy to counter disinformation during the war, combining government coordination, civil society engagement and technological innovation. Institutions such as the Centre for Strategic Communications and the International Centre for Combating Disinformation are leading efforts to detect and debunk false narratives, while initiatives like PR Army connect Ukrainian voices with global media to shape international understanding (Carvin et al., 2023). Technological tools, including AI-powered platforms developed by Ukrainian startups, are used to monitor influence operations and respond rapidly to emerging threats. Ukraine's strategic communication efforts target domestic audiences, Russian citizens, and the international community, with storytelling and emotionally resonant content playing a key role in maintaining morale and support (The Digital Forensic Research Lab, 2024). This is seen as an important element in maintaining the 'will to fight' in Ukraine.

*Ukraine has developed a comprehensive strategy to counter disinformation during the war, combining government coordination, civil society engagement and technological innovation. […] Technological tools, including AI-powered platforms developed by Ukrainian startups, are used to monitor influence operations and respond rapidly to emerging threats.*

Public-private cooperation has also been essential. Companies like Google and Cloudflare have supported Ukraine's digital infrastructure and helped disrupt Russian disinformation operations (Handler, 2023). The Kyiv StratCom Forum and similar platforms have emphasized the importance of media literacy, flexible communication strategies and cross-sector collaboration in building long-term resilience. One of the under-prioritized groups in efforts to raise disinformation awareness are people living outside large metropolitan areas. This is because most civil servants tend to be concentrated in capital cities (Kalenský & Hanhijärvi, 2025: 34). However, in Ukraine, the Ukrainian Centre for Strategic Communication offers training sessions on countering disinformation and communicating strategically also for local authorities. In its three years of existence, the School for StratCom programme ran 200 training sessions for 1,000 civil servants on both national and local levels (SPRAVDI, 2025).

Ukraine's model demonstrates that effective resistance to disinformation requires speed, adaptability and inclusive engagement, and thus offers valuable lessons for democracies facing hybrid threats and information warfare. In the following chapter, we focus on the Psychological Defence Agency in Sweden (MPF), with a description of the agency, focusing on the organizational structure, funding, governance, mandate and rationale. This provides a basis for an analysis in Chapter 6.

# 5. The Psychological Defence Agency in Sweden

The Psychological Defence Agency (*Myndigheten för psykologiskt försvar* – MPF) was established in Sweden in 2022, but the concept of psychological defence and awareness of its importance have been present in the Swedish public discourse for close to a century. The journal article 'A Genealogy of Swedish Psychological Defence: Information Influence as a Shifting Problem for Democratic Governance' by Hedvig Ördén (2025) examines the historical development and conceptual transformation of 'psychological defence' in Sweden. Using a Foucauldian genealogical approach, Ördén traces how the notion of 'information influence' has evolved from a Cold War-era security concern into a contemporary governance tool aimed at safeguarding democratic integrity.

Specifically, the first official government body tasked with Sweden's psychological defence was the Preparedness Committee for Psychological Defence, which was founded in 1954 in the early days of the Cold War. This body was eventually merged with others into the Directorate for Psychological Defence (SPF) in 1985, but from 2002 onwards, the responsibilities of this second body were subsumed by other government agencies.


Figure 1: Timeline of the 'psychological defence' concept in Sweden

In 2009, the Swedish Civil Contingencies Agency (MSB) was formed from the merger of the SPF and two other agencies and thus became the main government body responsible for civil defence and emergency management. The debate about Sweden's psychological defence, however, would continue following the occupation of Crimea and the outbreak of war in the Donbas in 2014. In 2015, the Swedish Total Defence model was re-established, and politician Hans Wallmark from the Moderate Party, which at the time was the main opposition party, wrote an opinion piece in *Svenska Dagbladet* where he argued that there was a need for Sweden to establish a new agency specifically for psychological defence.

This initiated a new debate on the topic, and eventually, the MPF was announced by Prime Minister Stefan Löfven at the conference *Folk och Försvar* in 2018.

## 5.1. Organizational structure and funding

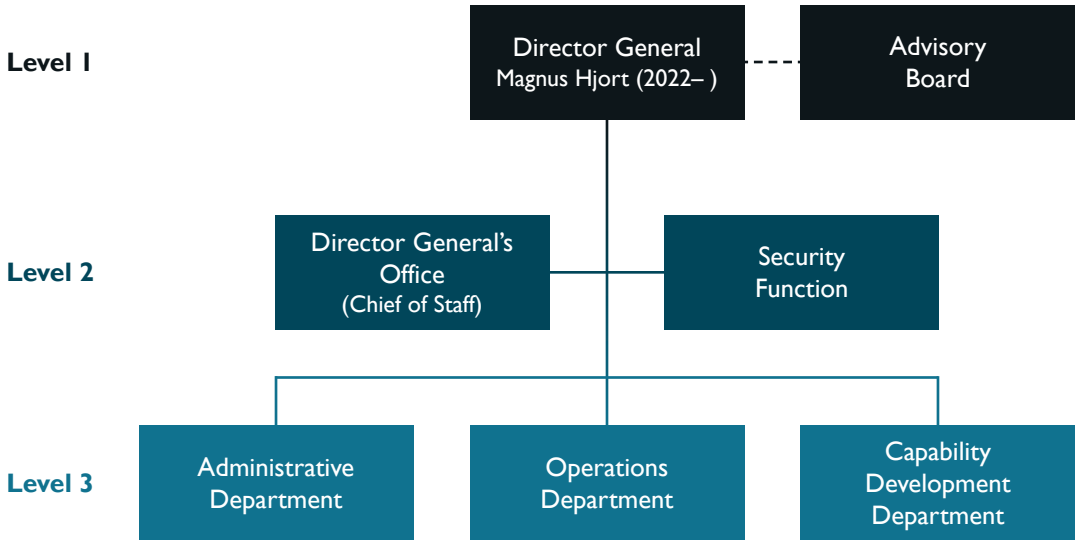


Figure 2: Organizational structure of the MPF

The organization of the MPF is rather unique in the European context, with the closest equivalent being the French model with Vignium. The organizational structure of the agency can be divided into three levels (see Figure 2). At the top of the organization sits the Director General (GD), who, since 2022, has been Magnus Hjort. The GD is also the head of the agency's Advisory Board, which is appointed directly by the government and serves to advise the GD and to evaluate the agency's work.

On the level immediately below the GD is the Director General's Office, which is headed by the Chief of Staff, and the Security Function, which is headed by the Chief Security Officer. Both these functions answer directly to the GD. Finally, on the third level are the three departments of the agency: The Administrative Department, the Operations Department, and the Capability Development Department. The latter are roughly the same size, but the Operations Department is marginally larger than the Capability Development Department. In the time since its inception in January 2022, the MPF has grown significantly and has almost doubled in size, with around 85 employees as per September 2025. The staff growth also includes several employees who are stationed internationally, such as at NATO Stratcom in Riga.

The preventive work on the capability development side involves strengthening societal resilience through information online and on social media. The agency is tasked with spreading knowledge, providing education and contributing to the preparedness of the public and relevant actors in matters of psychological defence. MPF also has a national responsibility for research, exercises and education in the field of disinformation and influence operations. Additionally, the authority engages

in extensive international cooperation, including through the secondment of national experts to the NATO Strategic Communications Centre of Excellence, the European External Action Service (EEAS) East StratCom Task Force, the EEAS Western Balkans StratCom Task Force, and through comprehensive bilateral cooperation, particularly with the United States and the United Kingdom.

When it comes to funding, Table 2 shows the income and expenses of the agency in the first three years it has been operational.[8]

| Line item | 2022 | 2023 | 2024 |
|---|---|---|---|
| **Income** | **113 195 (100%)** | **140 023 (100%)** | **155 658 (100%)** |
| Income by allocation | 111 296 (98%) | 135 487 (97%) | 151 178 (97%) |
| Income through grants | 1 845 (2%) | 3 481 (2%) | 3 705 (2%) |
| Other income (incl. financial) | 54 (0%) | 1 055 (1%) | 775 (0%) |
| **Expenses** | **113 196 (100%)** | **140 024 (100%)** | **155 658 (100%)** |
| Personnel expenses | 47 296 (42%) | 60 363 (43%) | 75 410 (48%) |
| Premises expenses | 4 418 (4%) | 4 849 (3%) | 5 161 (3%) |
| Other operating expenses | 58 559 (52%) | 70 328 (50%) | 69 403 (45%) |
| Financial expenses | 116 (0%) | 555 (0%) | 701 (0%) |
| Depreciation and write-downs | 2 807 (2%) | 3 929 (3%) | 4 983 (3%) |

Table 2: Income and expenses of MPF in the period 2022–2024 (thousands of SEK)

As the table shows, in the period from 2022 to 2024, more than 95% of the MPF's income came from government allocation, whilst less than 5% came from other sources. In the same period, the two largest expenses of the agency were personnel costs and 'other operating expenses', which together accounted for more than 90% of the costs in each year.

## 5.2. Governance, mandate and rationale

The Swedish government guides and administers the MPF through yearly directives in the form of appropriation letters. The instructions included therein set out the responsibilities and tasks of the agency, in addition to establishing what resources have been allocated to it and how these are to be used. The agency, in return, is responsible for delivering a budget appraisal every year for how it wants to run its operations in the coming three years, which serves as a basis for the allocation of funds by the government. Additionally, like all Swedish agencies, the MPF has a responsibility to hand in an annual report, every February, for the previous year, where expenses are accounted for and where the agency presents its progress towards the objectives set out in the appropriation letters from the government.

The base directives for the MPF were established in a government ordinance from October 2021, before the agency began its operations (Förordning 2021:936).[9] Therein, the government asserts that the objective of the MPF is to identify, analyse and provide support for countering influence operations, misinformation and disinformation directed at Sweden or Swedish interests. Through its operations, the agency should facilitate free and open discourse and defend democratic values and democratic society. Further directives are also laid out, which correspond with proposals from a committee report (SOU 2020:29); these will be discussed at greater length below (see also Table 3). An opinion poll published in 2025, which was conducted at the request of the MPF, found that 75% of Swedes think the MPF's tasks are important, and this has been steadily rising over the years that the MPF has been operational (MPF, 2025).

After the announcement by then Prime Minister Stefan Löfven in 2018 that a new agency was to be established focused on psychological defence, a government committee of inquiry, Psykförsvarsutredningen (PVU), was set up to investigate the need for such an agency, as well as the practical and rational basis for it. The result of this inquiry was presented by the committee in a report published in 2020, entitled 'A new agency to strengthen the psychological defence' (SOU 2020:29).[10]

Within this report, the PVU committee concluded that there was indeed a need for Sweden's psychological defence to be coordinated across different government departments and agencies, as well as to increase coordination between the state and private businesses and NGOs. The report argues that a modern psychological defence is faced with complex societal issues which span across widely different policy areas, and in order to facilitate its development and growth, coordinated cooperation across the whole of society is required. An agency tasked with psychological defence must further enhance the citizens' ability to discover and resist influence operations and disinformation campaigns. Thus, a robust psychological defence is seen as contributing to a more resistant citizenry and society, with a stronger 'will to defend'.

The report from the committee proposed seven main areas in which the new agency would operate, displayed below in Table 3.

| | Proposal from the committee report | Reasoning |
|---|---|---|
| 1. | In times of peace and in times of war, the agency is tasked with supporting, strengthening, coordinating and developing the joint societal resilience, within the realm of psychological defence. | According to the inquiry, it is unclear whether government agencies that have responsibilities concerning psychological defence are sharing enough information to perform their tasks capably. Instead, resources could be used more efficiently for coordinating the work of different agencies, especially in times of crisis. |

Table 3: PVU report, proposals and reasoning

| | Proposal from the committee report | Reasoning |
|---|---|---|
| **2.** | The agency is tasked with identifying, analysing and countering malign influence campaigns, and other dissemination of false or misleading information directed at Sweden or Swedish interests at home and abroad. | The inquiry finds that even during the period when it was carried out, when Sweden was not yet a member of NATO and nominally at peace, undue influence campaigns and the spreading of misleading information occurred frequently. This was a change from the Cold War, when this was not considered to be a large enough threat in times of peace to warrant an agency dedicated specifically to countering propaganda and disinformation. |
| **3.** | The agency will contribute to educating and continuously sharing knowledge with other agencies and relevant actors in society in order to increase their preparedness in the realm of psychological defence. | The inquiry notes that there is a need and a desire in different sectors of Swedish society, including among agencies, municipal governments, companies, and NGOs, to have more extensive support than what was previously accessible, to counteract undue influence campaigns. |
| **4.** | The agency will ensure that courses and exercises are readily available for other actors who operate within the areas that the agency has responsibility for. | According to the inquiry's assessment, investments into disseminating knowledge and expertise in the field of counter-intelligence and psychological defence are integral to strengthening the resilience of the whole of society, and this task should be included in the mandate of the new agency. |
| **5.** | The agency is tasked with ordering, tracking and ensuring the quality of research and knowledge production in matters of psychological defence, as well as making this research and knowledge readily available to the public and other relevant actors. | The inquiry states that it is essential that the new agency have a mandate to initiate and finance research in areas relating to psychological defence, which previously had been the responsibility of the Civil Contingencies Agency (MSB). In addition to this, the agency must also be tasked with staying up to date with current international research on psychological defence, and to communicate this to society at large. |
| **6.** | The agency will support the media in identifying, analysing and countering malign influence campaigns, to the extent that such support is requested by the media. | In conversation with representatives from the media, the inquiry found that there may be a future need for the new agency to support and defend journalists and the media as an institution from threats and inflammatory rhetoric. In order to ensure the continued independence of the media, however, such support will not be imposed but instead only come at the request of the media organizations themselves. |

Table 3: PVU report, proposals and reasoning *(continued)*

| | Proposal from the committee report | Reasoning |
|---|---|---|
| 7. | The agency will supply the Swedish government with information and grounds for developing the nation's psychological defence capabilities both in times of peace and in times of war. The agency has an obligation to report to the government any intelligence relating to undue influence campaigns or other dissemination of false or misleading information which may be of relevance to Swedish national security interests, or that for other reasons needs to be known by the government. These reports will be carried out in such a way as the government decides. | According to the assessment of the inquiry, the new agency must be able to supply the government with an informational basis for the development of the national psychological defence. In times when the nation is under threat, the risk of war is high, or the nation is already at war, the agency will support the government and suggest actions and strategies which will reduce the ability of the hostile party to cause harm to the nation or national interests. |

Table 3: PVU report, proposals and reasoning *(continued)*

The establishment of the MPF in January 2022 had broad support and did not face significant political opposition in Sweden. It was framed as part of the re-launch of Sweden's Total Defence strategy from 2015 and was widely regarded as a necessary step to strengthen resilience against disinformation and foreign influence operations (Suliman, 2022). However, some criticism emerged in public debate. Concerns centred on the risk of the agency being perceived as a 'Ministry of Truth', potentially undermining freedom of expression and press freedom. Others questioned the broad definition of 'misleading information' and whether such a mandate could open the door to state overreach. In addition, Swedish media pointed out that no psychologists were employed at the time of launch, raising questions about the agency's name (Psykologtidningen, 2022). Thus, while the establishment of MPF was politically uncontroversial, it did spark some debate over key normative issues such as freedom of expression, state responsibility in the information domain, and the agency's public legitimacy.

## 5.3. The agency in action: The 'LVU' disinformation campaign

In the immediate aftermath of its establishment, several major international and national events occurred which the agency had to relate to. For example, the ongoing 'Infodemic' surrounding the COVID-19 pandemic, Russia's full-scale invasion of Ukraine, which in turn was followed by Sweden beginning the process of accession to NATO, and Swedish national elections which took place in September 2022. One concrete example of where the MPF's operational department had to come into play during these years was to counter a disinformation campaign which first emerged in 2021 and lasted until at least 2024. The core of the campaign consisted of videos which were circulated on social media that were alleged to show Swedish authorities 'kidnapping' Muslim children from their families, using the 'Care of Young Persons (Special Provisions) Act' (LVU) as a pretext.[11] These videos originated from domestic Swedish accounts but were then spread more broadly by actors outside Sweden, most prominently by Egyptian influencer Shuoun

Islamiya, which amplified the negative impact the campaign had on the reputation of, and trust in, Swedish authorities (Ahlerup & Ranstorp, 2023).

> *The 'LVU' campaign consisted of videos which were circulated on social media that were alleged to show Swedish authorities 'kidnapping' Muslim children from their families, using the 'Care of Young Persons (Special Provisions) Act' (LVU) as a pretext. These videos originated from domestic Swedish accounts but were then spread more broadly by actors outside Sweden, most prominently by Egyptian influencer Shuoun Islamiya.*

The campaign had two target audiences; on the one hand, it was directed towards domestic Swedish audiences, especially first or second-generation immigrants from predominantly Muslim countries, with the purpose of eroding trust in Swedish authorities and Swedish society. On the other hand, the campaign was directed towards audiences abroad, again in predominantly Muslim countries, supported by posts containing the videos and false information primarily being circulated by Arabic- and Turkish-language accounts. The targeting of this secondary audience had the effect in 2022 and 2023 of creating a sort of rift between Sweden and countries with a majority Muslim population, in particular Türkiye, which led to a slowing down of Sweden's accession into NATO; the Swedish application was at the time still awaiting ratification from the Turkish parliament and President Erdoğan.[12] The so-called 'LVU' campaign also took place in parallel with the more widely publicized Quran burnings in Sweden, which occurred throughout 2023 and which were used by different actors to establish the image of Sweden as an Islamophobic nation. Commenting on this case and the related challenges, Anton Lif, a senior adviser on Cyber Security and Total Defence at Combitech, states in an article by *Utsyn* that:

> Our society generally has problems understanding context, patterns, and cause and effect. It is a cognitive vulnerability. This has become very clear in crises such as the corona pandemic and the Quran burnings in connection with the NATO application. This vulnerability is exploited by antagonists for successful influence. *(Lif, 2024)*

The notion that such vulnerabilities constitute fertile ground for successful malicious influence campaigns is supported widely in research, and the 'LVU' campaign revealed how these vulnerabilities can provide openings for foreign influence operations which can have damaging implications for Swedish society. The 2023 report by Ahlerup and Ranstorp mentioned above investigated the larger context in which this campaign took place, also considering the Quran burnings that took place throughout 2022 and 2023, and which resulted in the so-called 'Easter riots' in the spring of 2022. The conclusions from the report make it clear that these two separate campaigns have together led to a change in the threat picture both from outside actors and from within Sweden (Ahlerup & Ranstorp, 2023).

The same report further states that the newly founded MPF likely had a significant impact on the Swedish state's ability to contextualize and communicate a common situation report to the public regarding what was currently happening during the various stages of the campaign, as compared to a hypothetical scenario where the campaign had taken place before the establishment of the MPF. Having one authority responsible for making public statements and continuously providing the public with situation reports likely helped to reduce what was a great deal of pressure on individual social services offices, by creating an overarching situational picture across agencies and identifying priorities and appropriate measures (Ahlerup & Ranstorp, 2023: 189). In other words, strategic and well-crafted public communication was a key factor for limiting the damaging effects of the campaign. The authors also describe this case as an example of the fact that today's threats and challenges to democratic societies in a globalized information environment are increasingly cross-sectoral and that the distinction between what is legitimate and illegitimate, as well as internal and external, tends to be extremely diffuse, which places new demands on collaboration within government and municipal operations (Ahlerup & Ranstorp, 2023).

*Having one authority responsible for making public statements and continuously providing the public with situation reports likely helped to reduce what was a great deal of pressure on individual social services offices, by creating an overarching situational picture across agencies and identifying priorities and appropriate measures.*

Somewhat similar to the Swedish 'LVU-campaign', in 2016, Norway experienced a campaign targeting its child welfare services, *Barnevernet*. This led to international protests outside Norwegian embassies in over 20 countries, sparked by specific cases involving immigrant families. These protests were accompanied by emotionally charged narratives accusing Norwegian authorities of cultural bias and religious persecution. The campaign was amplified through information directed at diaspora communities, religious groups and foreign politicians, leading to diplomatic tensions and widespread media coverage. Much like the 'LVU' campaign, the *Barnevernet* controversy exploited cultural misunderstandings and misrepresentations of child protection laws. However, the Norwegian case was perhaps more fragmented and centred on individual incidents rather than a coordinated national narrative. While both campaigns illustrate how child welfare institutions can become targets of disinformation and influence operations, they also highlight the importance of strategic communication and institutional transparency in maintaining public trust. Norway's experience underscores the need for resilience against emotionally driven and internationally amplified disinformation, especially in cases where disinformation or harmful narratives could ultimately lead to a worsening of the national security situation.

# 6. Analysis and findings

Although Norwegian authorities have taken steps to counter the spread of disinformation, primarily via efforts to strengthen media literacy and source criticism (see e.g. Meld. St. 5, 2020–2021: 95–101), pending the implementation of the 2025 national strategy against disinformation, the approach to increasing societal resilience to disinformation still appears less explicitly articulated than in neighbouring countries such as Sweden and Finland. This is underlined also by Bergaust et al. (2022).

While the previous chapters have focused mainly on empirical insights, in the following, we will draw on some theoretical insights from research on this topic. After presenting a brief state-of-the-art, we will share some selected findings from a two-part survey designed to improve the understanding of public perceptions, trust and behaviours related to disinformation in Norway. Against this background, we examine some of the main differences between the Norwegian and the Swedish approach to institutionalizing resilience. We also summarize the main challenges going forward, providing the basis for the recommendations in Chapter 7.

## 6.1. Research state-of-the-art

In the past decade, research on disinformation, its consequences and how to prevent it has seen an uptick, due to many of the factors which have been discussed in this report: the rise of social media, the COVID-19 pandemic, the increased geopolitical contestation between Russia and NATO countries/allies, and the polarization of politics in the West. This section will seek to summarize some recent research from Europe and more broadly on how disinformation can be combatted and how resilient populations can be built.

Firstly, also in the research field, there seems to be a focus on efforts to fight disinformation, rather than to define it. As an indication of academic priorities, a Google Scholar search (November 2025) for 'combat disinformation' yields 4,650 entries; this contrasts with 1,020 for 'identify disinformation', 257 for 'expose disinformation' and 101 for 'analyse disinformation'.[13] However, several research articles provide examples of the difficulty in fighting disinformation with facts, fact-checking initiatives and increased media literacy. First, in an article from 2018 titled 'The spread of true and false news online', Vosoughi et al. demonstrate how untruth is spreading faster, deeper and more efficiently online than truth. To arrive at this conclusion, the authors investigated the differential diffusion of all the verified true and false news stories distributed on Twitter from 2006 to 2017, with data comprising ~126,000 stories tweeted by ~3 million people more than 4.5 million times. Their findings show that false news stories tend to be more novel than true ones, and people tend to share novel information at a higher rate than information not considered novel. Interestingly, they also found that bots share true and false rumours at approximately the same rate, meaning that false rumours being more widely circulated cannot necessarily be attributed to bots.

Similarly, Buchanan (2020), in the peer-reviewed article 'Why do people spread false information online? The effects of message and viewer characteristics on self-reported likelihood of sharing social media disinformation' found that individuals are more likely to share disinformation when it aligns with their pre-existing attitudes, even when they recognize it as false. The study highlights that consistency between message and recipient beliefs significantly influences the likelihood of sharing, suggesting that motivations such as reinforcing identity or provoking reactions can override concerns about accuracy (Buchanan, 2020). In other words, information we agree with, that we want to use to stage a certain impression of ourselves, or information we think can be used to purposely provoke our audience are deciding factors when we consider whether to share information online. The authenticity of the information is not.

This is further reflected in findings by Pennycook et al. (2021), who describe how, even when someone knows that something is untrue, this does not in itself keep them from sharing this piece of information. Their research shows that '(...) people often share misinformation because their attention is focused on factors other than accuracy, and therefore they fail to implement a strongly held preference for accurate sharing' (Pennycook et al., 2021). Ultimately, however, the authors conclude that minor interventions are enough to 'nudge' users towards prioritizing accuracy. Research from the psychology field, conducted by Jon Roozenbeek and Sander van der Linden (2019) takes on a more experimental approach, in the form of a large-scale experiment involving 15,000 participants. These research subjects participated in a 'game' where they took on the role of producers of fake news and were taught six different strategies and techniques that are commonly used in the fabrication of news meant to mislead and deceive. The authors show that in a such a controlled setting, subjects improved their ability to detect fake news after being 'inoculated'. This finding was shown to hold true regardless of age, level of education, cognitive style or political ideology. The findings from Roozenbeek and van der Linden (2019) provide some evidence for the thesis that media literacy training and teaching the population about how fake news actors tend to operate on average contribute to increasing resilience and our ability to withstand disinformation campaigns.

Aside from the findings from the Hybrid CoE (Kalenský & Hanhijärvi, 2025) which have been presented previously, various other European organizations and institutions have released research and reports centred on countering disinformation and building resilient populations. A 2021 report from the European Digital Media Observatory (EDMO), for example, summarizes research done on media literacy in Europe and finds that, whilst media literacy is one key component to combatting disinformation and building resilience, it should not be seen in isolation, and expanding media literacy is thus not a 'silver bullet' for politicians who seek to find easy solutions for making their populations more resilient (Goodman, 2021).

In a different vein, a 2022 publication from the European Audiovisual Observatory investigates and connects the international frameworks that guide European responses to disinformation to the national responses of individual states in Europe, using legislative responses in Germany,

France, Italy and the UK as case studies (Cabrera Blázquez et al., 2022). Additionally, the authors bring up multiple examples of non-legislative methods used by European countries in order to combat disinformation, including government campaigns and media regulations; the examples introduced come from Iceland, Ireland and Norway. The Norwegian example relates to the SMS-campaign launched by the Norwegian Media Authority (*Medietilsynet*) in 2019, called '*Stopp. Tenk. Sjekk.*' ('Stop. Think. Check.'). In short, during this campaign, many Norwegian residents received an SMS that contained an exercise aimed at making the recipients stop and think for a few moments after seeing a news headline, before asking them simple questions to help them reflect on their own reaction to it. This campaign has since been shared with authorities in other European states and has also served as an inspiration for a very similar campaign a year later in Iceland (Cabrera Blázquez et al., 2022).

*[D]uring [the Norwegian Media Authority's 'Stop. Think. Check.'] campaign, many Norwegian residents received an SMS that contained an exercise aimed at making the recipients stop and think for a few moments after seeing a news headline, before asking them simple questions to help them reflect on their own reaction to it. This campaign has since been shared with authorities in other European states.*

In summary, research conducted in this field largely points to individuals and social media users being important agents when it comes to the spread of disinformation, 'fake news' and other types of false information. The research also finds, however, that relatively minor interventions and 'nudging' users in different ways can sometimes be enough to adjust sharing behaviours and to enable individuals to detect false information. For example, the campaign by the Norwegian Media Authority mentioned above helped to inspire part of a research project on trust and behaviour around disinformation, which will be presented in the next section.

## 6.2. Public perceptions, trust and behaviours around disinformation

As shown in this report, the era we live in is marked by rapid information flows and increasing digital manipulation. For resilience-building efforts to be effective, it is therefore critical to understand how individuals perceive and relate to disinformation. In the following, we present some selected findings from a two-part survey conducted in 2024 to assess public attitudes as well as behavioural and emotional responses to false news headlines and disinformation, both before and after a targeted SMS-based educational intervention. The content of the SMS messages was largely based on the 'Stop. Think. Check.' campaign by the Norwegian Media Authority (*Medietilsynet*). The survey was funded and carried out in the context of the research project 'Disinformation and people: impacts on societal trust and resilience (FAKENEWS)'. The project is led by Professor Gunhild Hoogensen Gjørv at the University of Tromsø. Senior Researcher Stine Bergersen, main author of the current report, led PRIO's part in the project.[14]

The research consisted of two separate online surveys, with an SMS intervention in between. The first survey aimed at mapping e.g. online behaviour, media use and trust. After receiving the SMS intervention, the second survey aimed at seeing whether there were changes in terms of respondents' ability to detect fake news headlines etc. A representative selection totalling 6,561 individuals responded to the initial survey conducted between 10 February and 6 March 2024. Of these, 3,495 participants agreed to continue with the study and receive ten SMS messages over a period of five weeks as part of the intervention. 3,449 responded, but some reported not receiving the SMS messages and some withdrew during the intervention, resulting in a final sample of 2,276 Norwegian participants who received the intervention and completed both surveys. The results reveal some patterns in media trust, crisis communication preferences, emotional impacts of news, and the perceived responsibility for combatting disinformation. Notably, the educational element of the SMS intervention led to modest but meaningful improvements in participants' confidence in recognizing disinformation and their tendency to verify emotionally charged news.

The first survey indicates that, in times of crisis, people tend to rely most on their personal networks, with 41% indicating they would turn to family for information. Furthermore, the police and emergency services, DSB/FHI[15] and other state agencies, as well as NRK and NRK Radio were indicated by respondents as being trusted sources of information in an emergency. Schools were identified as the least likely source of crisis-related information, with only 2% of respondents saying they would be most likely to turn to schools for information in such a situation, and 45% stating it is the source they would least likely turn to (see Figure 3).

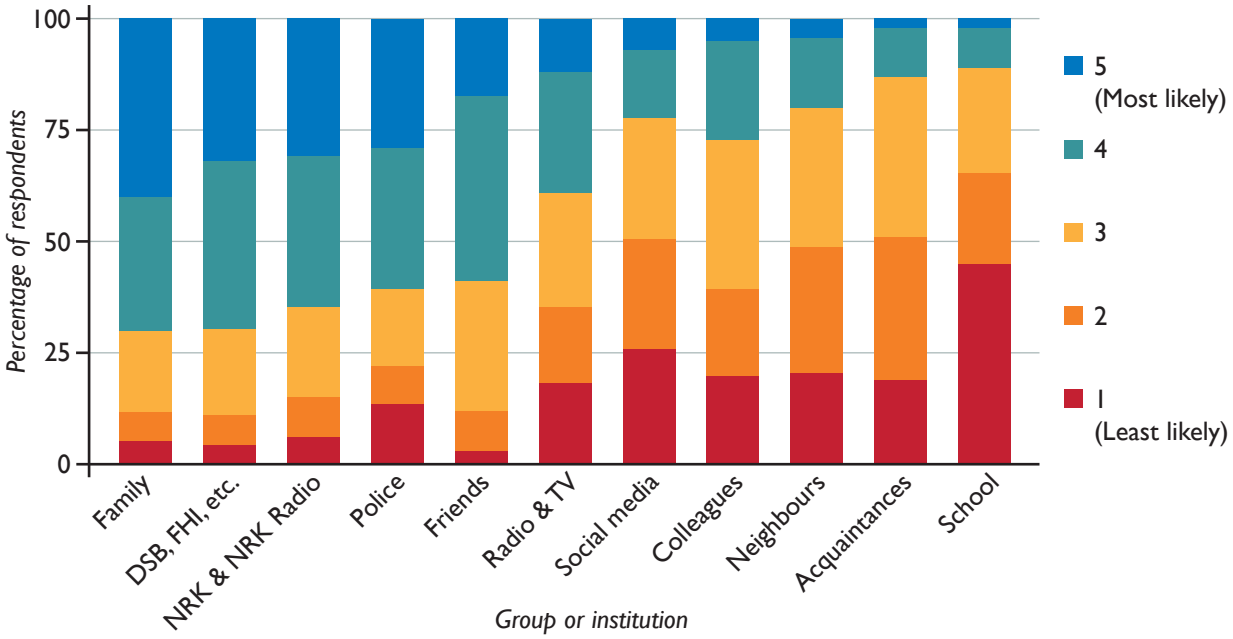


Figure 3: Different groups and institutions ranked by how likely respondents are to turn to them in the event of an emergency[16]

When it comes to media usage and trust, NRK TV/Radio stands out as being both widely used and highly trusted. 81% of respondents said that NRK is one of their main sources for news, and 68% said NRK is the news source they have the highest trust in. This can be compared with the second most trusted news source, nationwide newspapers, which only 10% of respondents said they trust the most. Despite this high trust, only 29% of respondents said they would be most likely to turn to NRK for information in the event of a crisis, as can be seen in Figure 3.

Another interesting finding is that consuming news through NRK TV and NRK Radio is high amongst all groups, but most common for people who have completed four or more years of university; in this group, 88% of respondents said that NRK is one of their main sources for news. The same percentage for the category of respondents who have only completed secondary school is 74%, and the results indicate that, as education decreases, so does the share of respondents who use NRK (see Figure 4).[17] In the same way, trust in NRK and NRK Radio was also found to be higher among respondents with longer education. Among participants with four or more years of university education, 73% reported that they had the highest trust in NRK, out of all possible news sources they had to pick from; the same statistic was 61% for respondents with only a primary school education.

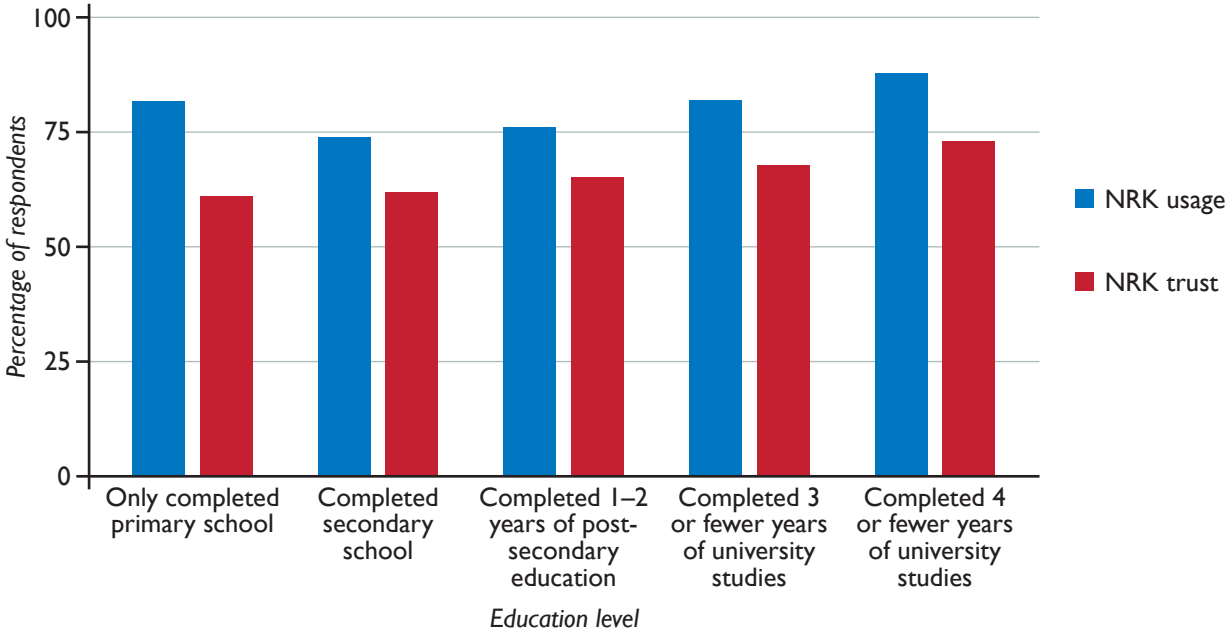


Figure 4: Usage of NRK and trust in NRK, based on education level

Among social media and other 'non-traditional' forms of media, a plurality of respondents (37%) reported using Facebook as one of their main sources of news, which was followed by Instagram at 18%. Out of all the respondents, 38% state that they receive none of their news from any of the listed non-traditional media platforms. These results were also found to be correlated with level of education. Among respondents who had completed four or more years of university, only 28%

claimed to get their news from Facebook. The number of respondents claiming to get their news from Facebook rose to 43% among those who had only completed secondary school. When asked which news source they had the least trust in, 26% of respondents said Facebook and 27% said TikTok, regardless of education level.

Most participants reported reading news in Norwegian, indicating a strong preference for native-language content. In terms of sharing behaviour, 45% of respondents said they did not share news at all on social media, a percentage that remained unchanged after the intervention. However, there was a slight increase in those who reported sharing news a few times a year, rising from 39% before the intervention to 43% afterward.

Emotional responses to news, such as feeling upset, fearful, sad or happy, remained relatively stable across both surveys. Nonetheless, there was a modest post-intervention increase in participants' tendency to verify news that provoked emotional reactions, along with a slight decrease in their likelihood of sharing such content. These patterns suggest that while emotional impact remained consistent, the intervention may have encouraged more cautious and reflective behaviour in response to emotionally charged news.

| Response category | First survey | Second survey |
|---|---|---|
| 1 Do not agree at all | 1% | 1% |
| 2 | 2% | 1% |
| 3 | 7% | 5% |
| 4 | 23% | 19% |
| 5 | 33% | 38% |
| 6 | 21% | 28% |
| 7 Agree completely | 5% | 7% |
| Don't know / don't want to respond | 7% | 2% |

Table 4: Shares of how respondents in each survey rated the statement: 'I am able to detect untrue news in traditional or social media'

After the SMS-intervention, which consisted of ten SMS messages being sent out over a period of five weeks, the follow-up survey showed that respondents' belief in their own ability to recognize fake news increased: in the first survey, 59% of respondents rated their own ability to detect false headlines a 5 or higher on a 7-point scale; in the second survey, this number had risen to 73%.

Both surveys included a section where participants were presented with ten headlines (half of which were actual news headlines, and half of which were fabricated) and asked to rate these on a

6-point scale based on credibility, where 1 was 'very untrustworthy' and 6 was 'very trustworthy'. The false headlines were consistently viewed with scepticism, with 64–79% of respondents in the first survey giving them a score of 3 or lower. In the post-intervention survey, this number was 62–93%, which provides weak evidence that respondents managed to better identify some false headlines. Verifiably true headlines were generally rated as moderately trustworthy in the first survey, with 49–83% of respondents assigning them a score of 4 or higher; in the second survey this number rose significantly to 76–89%. However, one true headline in the second survey, stating that the Swedish government was investigating options to increase emigration, was mistrusted by a majority (71%) of respondents, highlighting the challenges in public discernment even when information is accurate.

While the first survey did not mention the term 'disinformation' at all, in the follow-up survey, some additional questions were asked regarding disinformation specifically. When asked how often they believe they encounter disinformation, 33% of respondents stated the belief that they see disinformation a few times per week, whereas 19% believed it to be more frequent than that, and 42% believed it to be less frequent. Further, when asked who should bear the greatest responsibility for combatting disinformation, most respondents replied that this burden should fall on traditional media (58%) and on the government and politicians (57%).[18] Schools and educational institutions, alongside organizations and public authorities, were both rated as most responsible by 46% of respondents. 39% believed individuals themselves carry the greatest responsibility to combat disinformation, whilst the least amount of people (31%) believed that social media companies should bear the greatest responsibility (see Table 4).

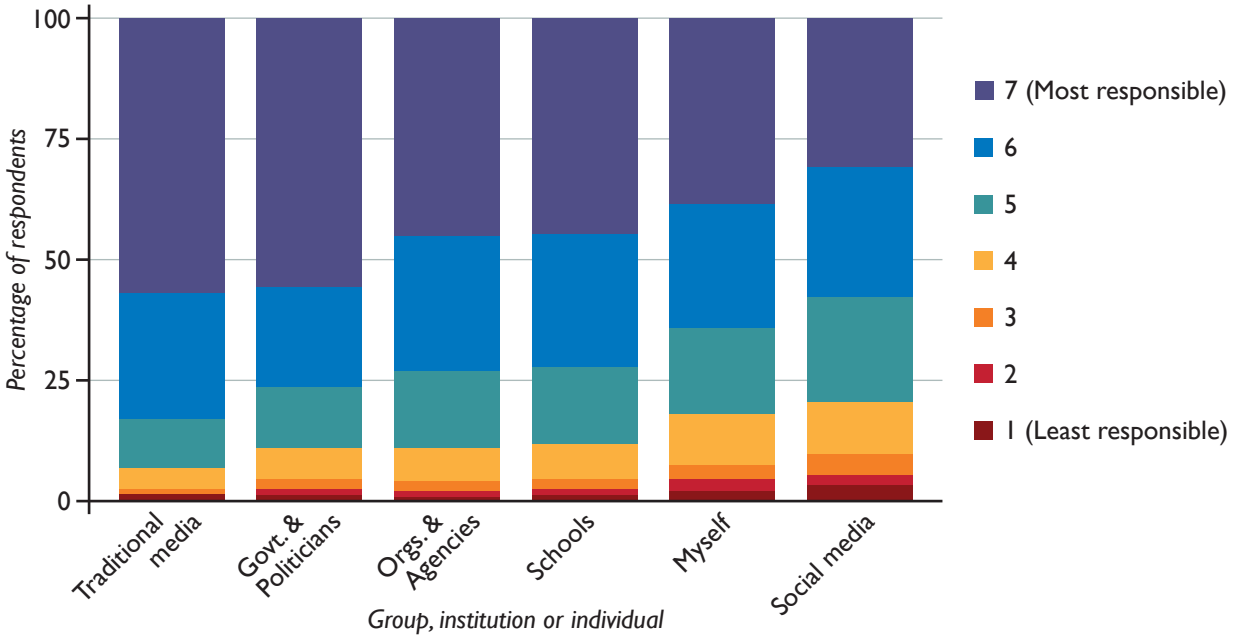


Figure 5: Who do you see as being responsible for countering disinformation?[19]

In sum, seen together, these insights offer valuable implications for designing effective public resilience strategies and enhancing psychological defence mechanisms in the face of such threats. For example, they suggest that it might be valuable to consider where people tend to turn for information during a crisis, what the level of trust in different institutions are, where and how people read news, and what their social media behaviour generally is.

Following the SMS intervention, several subtle but meaningful behavioural shifts were observed that may be of relevance to the MoD. Participants showed an increased tendency to verify emotionally charged news before sharing it, suggesting a growing awareness of the risks associated with impulsive information dissemination. There was also a small but consistent rise in the number of individuals who chose not to share news after experiencing emotional reactions, perhaps indicating a more cautious approach to online engagement. Importantly, the intervention led to improved recognition of false news, with more participants expressing confidence in their ability to identify disinformation. This heightened awareness was accompanied by a clearer perception of how frequently disinformation appears in their media environment, with a third of respondents reporting they encounter it several times a week.

Another important insight from the surveys has to do with responsibilities. When asked who should bear the greatest responsibility for combatting disinformation, respondents overwhelmingly pointed to traditional media and government institutions. This reflects a strong public expectation that official channels and authorities should take the lead in safeguarding the information space. For the MoD, these findings might allude to the importance of coordinated communication strategies and public education efforts as potential parts of a broader psychological defence framework.

*When asked who should bear the greatest responsibility for combatting disinformation, respondents overwhelmingly pointed to traditional media and government institutions. This reflects a strong public expectation that official channels and authorities should take the lead in safeguarding the information space.*

## 6.3. Institutionalizing resilience

Equipping citizens with the tools to recognize and critically assess false information, and engaging with citizens (such as through SMS campaigns) can directly contribute to the psychological and informational dimensions of the total defence concept. Such engagement can help ensure that the population remains informed, vigilant and less susceptible to harmful manipulation, which in turn strengthens national preparedness and response capacity. And ultimately, such trust-building efforts can positively impact the will to defend.

Sweden's psychological defence strategy represents a significant evolution from traditional security measures to a comprehensive democratic governance framework. The approach can be described as proactive, institutionalized and rooted in liberal values such as transparency and civic empowerment. Norway, while responsive to threats similar to the 'LVU- campaign', so far maintains a more decentralized and less articulated approach, generally founded on the principles of responsibility, equality, proximity and cooperation (*ansvarsprinsippet*, *likhetsprinsippet*, *nærhetsprinsippet*, *samvirkeprinsippet*). The Swedish case offers valuable insights for countries seeking to balance national security with democratic integrity in the face of increasingly complex information environments. In the following, we will identify some main lessons learned from Sweden, which could be relevant for future efforts in Norway.

*Sweden's psychological defence strategy represents a significant evolution from traditional security measures to a comprehensive democratic governance framework. The approach can be described as proactive, institutionalized and rooted in liberal values such as transparency and civic empowerment.*

### 6.3.1. Lessons learned from Sweden

As shown, initially, psychological defence in Sweden was framed as a response to Soviet propaganda, with a focus on protecting national sovereignty and public morale. Over the decades, as we have seen, the concept has expanded to address a broader range of threats, including digital disinformation, foreign influence operations and domestic polarization. The previously mentioned research article by Ördén (2025) argues that psychological defence has shifted from a military and intelligence function to a mechanism of democratic governance, emphasizing transparency, civic resilience and public trust. It was this transformation which culminated in the establishment of the Swedish Psychological Defence Agency in 2022.

As described above, the agency is tasked with coordinating the national efforts to counter disinformation and influence campaigns, while also promoting media literacy and critical thinking among citizens. According to Ördén, this institutionalization in Sweden reflects a broader trend in liberal democracies, where psychological defence is increasingly seen as essential to maintaining democratic stability in the face of evolving information threats (Ördén, 2025). When Sweden frames psychological defence as a civic responsibility, closely tied to national security and democratic stability, it emphasizes not just fact checking, but also building trust, mental preparedness and societal cohesion.

*Ördén (2025) argues that psychological defence has shifted from a military and intelligence function to a mechanism of democratic governance, emphasizing transparency, civic resilience and public trust. It was this transformation which culminated in the establishment of the Swedish Psychological Defence Agency.*

The focus on democratic values is echoed by Mikael Tofvesson, head of MPF's operational department, who describes the agency's approach to defining threats versus vulnerabilities:

> It is important to stress that the agency counters only foreign disinformation and this is done strictly for democratic reasons. As a defence organization, our operations could not be used against our own population. People who spread disinformation in our societies are perceived as a vulnerability and not as a threat. A vulnerability is someone who needs help and support to make them resilient against the threat of foreign actors such as Russia, which spread disinformation that we need to counter. The agency can expose these disinformation narratives and use any tool to counter them and strike back. Therefore, we have this perspective: internal disinformation is a vulnerability, while external disinformation is a threat. *(New Eastern Europe, 2024)*

Here, Tofvesson underlines how the MPF only counters foreign disinformation for democratic reasons and never targets its own population. Domestic actors spreading disinformation are seen as vulnerabilities needing support to build resilience, whereas foreign actors like Russia are considered threats.

Looking forwards, to achieve a further strengthening of Sweden's psychological defence, even better cooperation and coordination among all involved actors is necessary, according to a 2023 report. The report states that, as of 2023, the current level of cooperation and coordination in Sweden on this area is still considered insufficient to achieve robust resilience at the national level. In the report *Structure for Effective Collaboration for Psychological Defence (Struktur för effektiv samverkan för det psykologiska försvaret)* (MPF, 2023), the MPF proposed a new structure for effective cooperation for psychological defence. The vantage point of the report is that psychological defence is intended to strengthen overall national defence capability, resilience and the will to defend. To achieve this, a flexible structure for cooperation is needed, one that enables collaboration across both military and civil defence, as well as with actors outside the formal civil preparedness system. Such a structure should also allow for the inclusion of relevant authorities or organizations when their involvement is necessary, either for preventive efforts or in the operational handling of hostile information influence against Sweden. Therefore, the MPF proposed establishing a *Cooperation Council for Psychological Defence*, supported by dedicated forums, to ensure effective collaboration in Sweden. The council should include representatives from the Armed Forces, the Security Police, the Civil Contingencies Agency (MSB), the county administrative boards, the Authority for Press, Radio and Television, the Swedish Media Council and the Swedish Institute. The purpose of this cooperation council would be to further improve coordination between actors, enhance joint operational capability and create synergies. Through the exchange of experience and increased awareness of each other's roles, participating actors can help ensure that psychological defence work is effective, sustainable and guided by a shared, long-term perspective.

*[The Swedish Psychological Defence Agency] only counters foreign disinformation for democratic reasons and never targets its own population. Domestic actors spreading disinformation are seen as vulnerabilities needing support to build resilience, whereas foreign actors like Russia are considered threats.*

A focus on cooperation and coordination is present in most discussions and discourses about various ways of institutionalizing psychological defence. The report by Ahlerup & Ranstorp (2023), whose task was reviewing the agency's handling of the 'LVU- campaign', also underlines the need for better coordination as a way of addressing the root causes that enable disinformation to spread. They write that '[i]t is also crucial to ensure coordinated efforts against various forms of information influence campaigns and disinformation targeting Sweden', and further that '[i]t is not sufficient for several authorities and municipal bodies to be given the specific task of increasing their focus on countering disinformation', but that '[t]his must be combined with a comprehensive focus on preventive work addressing the underlying factors that allow such campaigns to gain traction and spread in Sweden' (Ahlerup & Ranstorp, 2023: 193). According to the authors, this includes increased confidence-building measures between citizens and Swedish public administration. Ahlerup & Ranstorp (2023) are also clear that focusing solely on disinformation without allocating resources to long-term preventive and trust-building efforts would signify addressing only the symptoms, rather than the underlying causes of today's existing threats and challenges. They conclude that the 'LVU- campaign' clearly exposed a significant vulnerability in Swedish society, namely the lack of trust between government authorities, municipal services and certain groups of citizens.

Related to this is the issue of responsibilities, especially seen in relation to trust and legitimacy. Clarifying roles and responsibilities has been important in the Swedish context, also as a way of limiting misrepresentations of the agency's role and mandate. For example, according to Director General of MPF, Magnus Hjort, it is essential for the MPF in their public communication to continue to be clear that the aim of the agency is not to monitor its own citizens. Hjort referred to the 'F' in FIMI as highlighting this important distinction. As we have seen, for the MPF, while the spread of disinformation by domestic actors is considered a vulnerability, disinformation originating from foreign sources is considered a threat. This reflects the fact that the national population is to be considered vulnerable if they are not source-critical and vigilant, and if they lack knowledge about what might threaten them.

Furthermore, engaging with the public is underlined as important, and strategic communication is also highlighted by Hjort. This is also evident in the 2024 report *Opinioner* by MPF, which examined how Swedish citizens view issues related to security and defence, with a focus on their willingness to engage in total defence and their perceptions of Sweden's defence capabilities and preparedness in crisis situations (MPF, 2024). By analysing attitudes and values related to defence

and security in Sweden through such annual reports, the MPF generally gain a deeper understanding of how the population perceives Sweden's security policy, as well as their expectations and concerns regarding future crises or conflicts. Part of this is also an investigation of the extent to which citizens are prepared to take responsibility and contribute to the country's defence in a potential wartime situation.

Public awareness about the MPF is not necessarily a requirement for its measures to be successful, but it might indicate their level of public outreach and communication. In the most recent report from 2024, we see that 47% of the Swedish population are aware of the existence of the MPF, which is a slight increase compared to 43% in 2023. Among those who are aware of the agency, a larger proportion are men and older individuals. 75% believe that the agency's mission is important in 2024, compared to 70% in 2023. Among those who consider the agency's mission important, the largest proportion are individuals between the ages of 65 and 74 years (87%) and people educated at university level or higher (79%).

Hjort further highlights the following as key experiences since the agency's establishment, which could provide valuable lessons for Norway.

1. There is a need for more knowledge and an improved approach when it comes to **data protection and privacy**, and issues related to GDPR.
2. The importance of **strategic communication with the public** is emphasized, and it is acknowledged that this area requires further investment. This is also evident in the 2024 *Opinioner* report (MPF, 2024).
3. The role of research and its support in the agency's work have become even more critical than at the time of MPF's inception. **There is a demand for research on the different variables impacting the will to fight/to defend**, on the **relevant threat actors** (such as the research report *Doppelgänger*), and there is a need for more research on **which factors contribute to increasing resilience** (what works, and what does not work).
4. There is ongoing reflection on **the size of the agency**. While the demand for MPF's services and expertise far exceeds its current capacity, there is also consideration of whether the current size is appropriate, with reference to the fact that a significantly larger organization could introduce new challenges.
5. Careful consideration is encouraged regarding the **geographic location** of a similar agency in Norway. MPF is based in Karlstad and Solna, but given the mandate of the agency, accessibility for both domestic and international visitors is seen as important, potentially suggesting a more central location would be advantageous. This indicates a need to ensure balance between regional policy considerations and operational effectiveness.

6. **The importance of a shared conceptual framework** is underscored, both internally and in collaboration with international partners. There is value in debating and discussing the terms used, as this current report in itself seeks to do. Hjort points in particular to the EU term FIMI (Foreign Information Manipulation and Interference) as an example of constructive terminology, as it clearly defines the agency's mandate in addressing external influence.

In addition, in the report by Pammant & Isaksson (2024), prospects for further developing Swedish psychological defence are raised. When it comes to efforts targeting the domestic population, focusing on strengthening democracy, the following areas are mentioned as key:

- Understanding vulnerabilities.
- Strengthening institutions.
- Strengthening societal trust and the will to defend.
- Understanding social grievances and where possible encouraging mitigation.
- Educating, informing and empowering the public.

Also here, these priorities underscore that psychological defence is not only about countering external influence but also about reinforcing the internal foundations of democratic resilience. By addressing vulnerabilities, fostering trust in institutions, and empowering citizens through education and transparent communication, the idea is that societies can build a more robust defence against cognitive and hybrid threats. Sweden's experience illustrates the importance of institutional clarity, democratic safeguards and strategic coordination in building psychological resilience. The lessons outlined above range from structural cooperation to public engagement and the importance of research. For Norway, integrating these lessons into the total defence framework could contribute to improving social cohesion and enforcing a shared commitment to democratic values.

> *[P]sychological defence is not only about countering external influence but also about reinforcing the internal foundations of democratic resilience. By addressing vulnerabilities, fostering trust in institutions, and empowering citizens through education and transparent communication, […] societies can build a more robust defence against cognitive and hybrid threats.*

### 6.3.2. Norway's civil preparedness in uncertain times

As described in Chapter 4.1, Norway recently adopted two key national strategies: a strategy for building resilience against disinformation, and a national security strategy. The implementation and follow-up of both strategies is ongoing and is likely to imply significant structural changes over the coming years.

Such changes take place in uncertain times. A recent survey conducted by InFact on behalf of *Forsvarets forum* indicates that more than a third of Norwegians fear war. To the question, 'Are you afraid of war in Norway?', 35.1% answered 'yes'. This is an increase of 4.6% from the previous survey conducted in June 2024 and suggests that times are uncertain and that resilience-building efforts are of importance (Berggreen Kaalaas, 2025).

Civil preparedness is a foundational element of the total defence concept, which emphasizes that national security is a shared responsibility between military and civilian sectors. Civil preparedness ensures that public institutions, municipalities, private actors and the general population are equipped to respond to crises, ranging from military threats to cyberattacks and disinformation. Important components are for example coordination between civilian and military actors and trust-building between citizens and institutions. This integrated approach is designed to safeguard not only territorial integrity but also democratic values and societal stability.

The Norwegian government's White Paper on Total Preparedness (Meld. St. 9: 2024–2025) outlines three strategic goals for civil society: to be prepared for crisis and war, to withstand complex and hybrid threats, and to support military efforts through coordinated civilian action. The white paper also emphasizes the need for a culture of preparedness across all sectors of society, again highlighting that resilience must be built collectively, by individuals, municipalities, businesses and national authorities.

*A recent survey conducted by InFact on behalf of Forsvarets forum indicates that more than a third of Norwegians fear war.*

However, there are several reasons why Norway is already particularly well-placed to withstand the negative effects of disinformation. First, the education level is high. Second, there is a high level of trust in public institutions, government and politicians. Third, there is a strong presence of and trust in editor-based free media, which is often highlighted as the first line defence in this area. As highlighted also by Samuelsen (2023), according to a study by Humprecht et al. (2020), additional features of Norwegian society also strengthen the nation's collective resilience. For example, Norway's political multi-party system provides less fertile ground for polarization than a two-party system. Further, Norway's state-supported, editor-driven media ensure quality journalism as a counterweight to false content, which positively affects the collective robustness of Norwegian society.

On the other hand, the results from the survey by the FAKENEWS project presented in Chapter 6.2 show that 67% of Norwegians spend one hour or more every day on social media, and out of all respondents, only 38% report not getting any of their news from social media. This high level of social media use may in turn contribute to weakening Norway's societal resilience. Although, as Humprecht et al. (2020) point out, we can expect that countries with a high degree of robustness against disinformation will still be exposed to information shared with malign intentions.

Again, this recalls the distinction made earlier in this PRIO Paper between fighting the existence of disinformation and countering the adverse effects of it.

> *Norway is already particularly well-placed to withstand the negative effects of disinformation. First, the education level is high. Second, there is a high level of trust in public institutions, government and politicians. Third, there is a strong presence of and trust in editor-based free media.*

While the abovementioned features already make Norway robust to some degree, a recent report on Norway's total defence, released 21 May 2025 by the Office of the Auditor General, highlights several key concerns regarding Norway's preparedness for crisis and war (Riksrevisjonen, 2025). According to the report, existing plans and exercises do not actually adequately prepare civilian actors at the municipal and regional levels to respond to increased military demands. The Armed Forces are urged to communicate their needs and priorities more clearly to ensure effective coordination. Furthermore, the defence sector in Norway, and elsewhere, faces uncertain times when it comes to needs and priorities related to securing the civil population. In a recent analysis by FFI, several factors underpin the seriousness of the situation; there is a need for increased budgets, both with regards to human resources and equipment. This, however, is challenged by inflation, the weakening of the Norwegian currency, and hefty demands for military equipment all over Europe (Sundby Fallmyr et al., 2025).

We have previously defined psychological defence measures as measures and strategies aimed at protecting individuals, groups or societies from harmful psychological influences, such as manipulation, propaganda, disinformation and other tactics that can undermine mental resilience, trust and decision-making. Responsibility for such efforts is currently divided among several actors. The Police Security Service (PST) plays a key role in addressing illegal influence operations and can store publicly available data for analysis. The Directorate for Civil Protection (DSB) is e.g. responsible for coordinated crisis communication and strengthening public resilience, including through preparedness campaigns. The Norwegian Media Authority promotes media literacy and freedom of expression. Various defence sector entities monitor and research influence operations. Fact checking is primarily carried out by the non-profit organization *Faktisk*. The Norwegian Data Protection Authority and the Directorate for Education are behind the online resource www.dubestemmer.no, where students and teachers in particular can learn about privacy and digital judgment (NOU 2023:17). Other existing national efforts aimed at the public, such as media literacy training, public communication about current threats, and psychological first aid initiatives, are currently managed across multiple institutions, including the Red Cross, the education system, the Norwegian National Security Authority (NSM), and several ministries.

Recent developments, however, including increased awareness of hybrid threats and digital manipulation, seem to have prompted Norwegian policymakers to consider more coordinated

and integrated approaches. Reports from the Norwegian Defence Research Establishment (FFI) and the Ministry of Defence (2024) suggest a growing interest in cross-sectoral coordination and public engagement, potentially signalling a shift toward an approach more aligned with Sweden's (FFI, 2023; Ministry of Defence, 2024). Still, Norway's approach to psychological defence (and related efforts under any designation) differs significantly from Sweden's in both structure and emphasis. While Sweden has centralized its efforts through a dedicated agency, Norway's response still remains more fragmented. Based on the insights described so far in this report, the following section will outline some overarching challenges for Norway going forward in this field. These will form the basis for the suggestions provided in Chapter 7.

## 6.4. Main challenges going forward

As we have previously described, there is a distinction between countering disinformation – for example, actively working with replacing falsehoods with verified facts – and mitigating its negative effects, such as (re)building trust between citizens and the authorities or the state. These are related but fundamentally different tasks. As outlined in the preceding chapters, the complexity of concepts such as disinformation, misinformation and influence operations presents several challenges for efforts that fall under the scope of resilience-building or psychological defence.

Disinformation is typically defined by its intentionality. It is designed and distributed to deceive. While it may include fabricated content or the manipulation of factual information (what we have defined as malinformation), it is most commonly the *purpose* behind the dissemination that distinguishes disinformation from other forms of misleading or false content. We argue that defending against disinformation spread by malign actors with the intent to influence public opinion (as was the case with the 'LVU campaign' in Sweden) is not the same as responding to viral rumours or misunderstandings circulating among citizens. Although all these situations can come with harmful effects, the responsibility for mitigation differs across these cases. A core challenge for psychological defence efforts therefore lies in attribution, in the sense of knowing the true source and intention behind a certain piece of information. Without reliable intelligence about the origin of content, it becomes difficult to determine whether a certain issue constitutes disinformation. This uncertainty complicates efforts to build societal resilience against a threat that is often invisible or ambiguous. And although foreign actors usually play a role in disinformation campaigns, this is not always the case. A report from RAND Corporation emphasizes that while state actors like Russia, China and Iran do indeed engage in disinformation, much of the content is amplified or spread by non-state actors, including unwitting users, influencers and domestic political groups (Cohen et al., 2021). Here, foreign influence works by amplifying domestic narratives or exploiting existing societal tensions.

Therefore, based on what we have described in this report so far, some key challenges can be identified:

First, **identifying disinformation** remains a foundational task. On the national level, this requires for example fact-checking mechanisms, and on the individual level, this requires for example media literacy initiatives. However, as Hayward (2025) argues, the problem with disinformation is not always about truth versus falsehood; it is rather to be seen as a problem which involves multiple framings – epistemic, behavioural and security-related – each with its own implications and limitations. Furthermore, disinformation often operates in grey zones, where emotional framing and selective truths are used to manipulate perception. Also, significant resources are required to fact-check or attribute extensively.

Second, and more specifically, **distinguishing disinformation from misinformation** can be essential. This involves understanding whether content was fabricated with malicious intent, a task that requires intelligence and contextual analysis.

Third, resilience should also be built against **influence operations that do not rely on fabricated content** but instead amplify harmful domestic debates or misinformation originating from ordinary citizens. These campaigns blur the line between internal discourse and external manipulation and demonstrate how true information can also be weaponized. As Sivertsen (2024) notes, Russia's information strategy is not only about spreading its own version of the truth but also about creating doubt. By amplifying tensions and exploiting truthful content, adversaries can destabilize societies without relying on outright lies. The many drone sightings around several European airports in the autumn and winter of 2025 illustrate this dynamic: the threat lies not only in the drone itself but also in the confusion and uncertainty it generates.

Fourth, and partly for these reasons, **fact checking and media literacy efforts alone are insufficient**. As we have seen, research shows that individuals tend to knowingly share false information online simply because they want to, and that falsehoods tend to spread faster, deeper and more persistently than truths (Vosoughi et al., 2018). This may suggest that only fighting disinformation with facts may be an inherently limited strategy.

Finally, the current **lack of systematic coordination of national initiatives** to tackle the threat of disinformation and its harmful effects emerges as a more overarching important challenge, for Norway but also in other European contexts.

As a step towards responding to some of these challenges, the Norwegian National Security Authority (NSM) suggests that national efforts against influence operations should be coordinated within a single organization. This could ensure a unified approach to strengthening societal resilience and allow access to classified threat intelligence, enabling influence operations (including disinformation) to be understood as part of a broader pattern of composite means (*sammensatt virkemiddelbruk*). NSM recommends that such a unit be granted legal authority to collect open-source information and be tasked with coordinating and supporting other actors

involved in countering influence operations. A range of stakeholders may play important roles here, including from the education system, research institutions, media and civil authorities. The unit could also disseminate knowledge to the public, support decision-making across government sectors, and facilitate research and competence development in the area. Furthermore, the unit could serve as Norway's national contact point for international cooperation, including with the EU and NATO, particularly in areas related to social media regulation and emerging technologies such as artificial intelligence (NSM, 2023: 74).

Similarly, the Total Preparedness Commission (NOU 2023: 17) recommends the establishment of a national function with an overarching responsibility for understanding and countering the threat of information operations, with a focus on strengthening public resilience to disinformation. The Commission does not take a position with regards to where such a function should be placed but emphasizes that undue influence in the information domain often originates from state actors, and a national capability should therefore be centrally located. According to the Commission, it should not be placed within the traditional intelligence and security services (EOS), to avoid suspicion and perceptions of surveillance (along the lines of 'Ministry of Truth' allegations, which the Swedish MPF encountered during its inception). Instead, such a function should promote transparency and engagement with society at large. While the EOS services would still play an important role, they could be defined as one of several contributors. The Commission also points to the fact that different countries have chosen different models: the UK has placed such a function within the media sector, while Sweden has established a state agency under the government, alongside other civil agencies involved in total defence. Fundamentally, according to the Commission, a similar function in Norway should be set up so as to serve the interests of the population, the business sector and public authorities across all domains. It should enhance societal resilience, improve situational awareness and support international cooperation.

Importantly, by any designator, the design of psychological defence efforts must be carefully balanced against fundamental rights, including freedom of expression. It seems clear that the objective should not be to restrict lawful speech, but to inform the public about coordinated influence operations that undermine democratic discourse. However, based on insights from other European contexts, a model with a centralized coordinated unit also presents risks. As mentioned, a centralized agency could be perceived as a 'Ministry of Truth', potentially undermining its legitimacy and fuelling conspiracy theories, thereby undermining its own mandate. If such a unit is to be understood as taking control over narratives it may challenge democratic norms and freedom of expression. Moreover, such a unit could itself become a vulnerable target for cyberattacks or information warfare. There is also the risk that it may appear distant from local realities, whereas municipalities, schools and civil society actors are often better positioned to build trust on the ground. In addition, such efforts might be seen as overly top-down, reducing public engagement to passive information campaigns rather than fostering genuine dialogue.

# 7. Recommendations for strengthening societal resilience against disinformation

In this chapter, we will provide recommendations and point to questions and areas of relevance which we consider to be of importance for the Norwegian Ministry of Defence's current and future efforts to increase societal resilience to disinformation. These should be understood against the challenges pointed out in the previous chapter and as supplements or extensions of existing strategies and measures. Their fundamental purpose is to limit the negative and harmful effects of disinformation. Importantly, while we make recommendations and suggest areas of focus, we underline that these are not to be seen as definitive answers on how to best meet the threats of disinformation.

A starting point for this report has been that preventing the existence of disinformation is a different task than preventing or limiting its damaging *consequences* on society and individuals. It is the latter that this PRIO Paper and its recommendations aim to contribute to. Here, as defined in Chapter 3, resilience means focusing on three core elements: the ability for Norwegian society to *withstand* disturbance (i.e. disinformation) without collapsing, the capacity of Norwegian society to *adjust* and continue functioning under new conditions, and the ability for Norway to *evolve* into a more robust condition as a result of the disturbance (e.g. enforcing trust and other democratic values).

## 7.1. Societal values, shifting contexts and the need for a holistic approach

Efforts to counter disinformation, or increase societal resilience to it, must be carefully crafted so that they are based on and underscore the same democratic values we want to strengthen and protect. Any resilience-building effort should focus on buttressing democratic values while avoiding the amplification of polarization and the creation of new social divisions. As also highlighted by the Total Defence Commission, efforts should ensure that the population remain as unified as possible. Not in the sense that everyone must agree on everything, but that as many as possible should have a shared understanding of what is important to defend. According to the Commission, this is crucial for resisting disinformation, attempts to sow division, and exploitation of discord by foreign actors, and it helps foster the necessary willingness within the population to defend the nation (NOU 2023:14: 152–153).

In addition to the importance of protecting democratic values, two more issues can be highlighted.

First, the feasibility and success of having dedicated organizations or agencies for coordinating resilience-building seems to largely depend on the specific national context in which they operate. The Nordic countries generally enjoy a solid international reputation and are usually highlighted as role models when we look at all the indices on freedom of expression, and the level of social and political trust is very high (Nordforsk, 2025). Although the MPF in Sweden can be considered pioneers in establishing a public institution to combat disinformation and may provide

valuable methodologies, organizational structures and approaches, the suitability of these models for other governments is highly dependent on local conditions (Freihse & Bochert, 2024). The following recommendations acknowledge that adopting or changing strategies requires a careful and thorough evaluation, highlighting the contextual, cultural, political and social conditions in Norway. For example, even though Finland, Norway, Denmark, Sweden and Iceland share many of the same democratic values, they are also clearly different due to their social, cultural and political histories. Furthermore, according to Drazkiewicz,[20] leader of the Nordic Disinformation Resilience Network, this is true not only because the countries are different, but also because of their different geopolitical positions. Finland, for instance, has more at stake when it comes to Russian threats than Iceland (NordForsk, 2025). Such issues should obviously be considered when doing comparative studies.

Second, the responsibility of the MoD as part of the cross-sectoral effort of detecting and managing FIMI is described in Meld. St. 9 2024–2024 (*Totalberedskapsmeldingen*):

> The Ministry of Defence is responsible for influence operations directed at the defence sector, defence policy, and defence capabilities, or that in other ways may constitute a military threat to national security, as well as international defence cooperation in the area. *(Meld. St. 9 2024–2024: 99) (Authors' own translation)*

Given the cross-sectoral nature of hybrid threats and their effects, and the fact that such threats tend to blur the civil-military divide, it seems of great value that multiple actors and ministries engage in the topic of how to build and maintain resilient populations. In other words, a holistic approach seems appropriate. A key finding from the surveys presented in Chapter 6.2 is that when asked who should bear the greatest responsibility for combatting disinformation, respondents overwhelmingly pointed to traditional media and government institutions. This reflects a strong public expectation that official channels and authorities should take the lead in such efforts. As we see it, for the MoD, these findings might allude to the importance of coordinated communication strategies and public education efforts as part of a potential broader psychological defence framework.

The following recommendations assume and suggest a broad interpretation of the responsibility of the MoD, meaning that we see issues such as trust (interpersonal trust, wider societal trust and institutional trust), individual and societal resilience, and democratic values such as freedom of speech as relevant to the defence sector, defence policy and defence capabilities.

## 7.2. Recommendations for the Norwegian Ministry of Defence

A resilient Norwegian society is better equipped to withstand, adjust to and evolve in the face of complex and evolving threats. To effectively counter the negative effects of disinformation and

hybrid threats, it is essential that the overall resilience of society is prioritized and elevated as a strategic objective. The White Paper on Total Preparedness (Meld. St. 10, 2025) emphasizes the need for civil society to withstand hybrid threats and support military efforts through enhanced societal resilience. As two key lines of defence in this regard, referring to the framework by Kalenský & Hanhijärvi (2025), we underline **raising public awareness** and **reducing vulnerabilities** as two key elements to building resilience. Based on this report, such efforts would benefit from the following:

- Better coordination of national efforts.
- Improving the clarity of concepts and terminology.
- A prioritization of strategic and transparent communication.
- A focus on strengthening trust through increased public awareness.

### 7.2.1. Recommendation 1: Strengthen national coordination

There seems to be a need to improve the national coordination of efforts with regards to the negative impacts of disinformation, and a centralized unit dedicated to increasing public resilience against disinformation could offer advantages. It could create clearer lines of responsibility and improve coordination across sectors. Rather than fragmented efforts by multiple institutions, a central actor could consolidate initiatives, close operational gaps (and contribute to closing theoretical gaps), and ensure a more coherent strategy. It could also serve as a vantage point for developing specialized expertise in areas such as information warfare, media analysis, psychological defence and strategic communication. A unified voice could enhance clarity and consistency in public messaging, potentially contributing to a strengthening of public trust. On the international stage, such a unit could serve as a clear contact point for partners like the EU and NATO and enable faster, more effective responses to disinformation campaigns.

The overarching goal of a coordinating unit for psychological defence (under any designation) should be to strengthen individuals' trust in democratic institutions, in one another, and in a shared understanding of reality. This need is further underlined by the fact that the public now accesses news from an increasingly diverse number of sources (ref. Chapter 6.2). Efforts to achieve a shared understanding must be cross-sectoral, a principle reflected also in recent government strategies. The challenge of disinformation in the current digital and globalized society requires a coordinated and holistic response from all sectors, because its impact cuts through all layers of society as well as across sectors. It seems clear that the concept of psychological defence should be understood as a team effort. As highlighted by Lif (2024), thinking of this effort in terms of a 'Quadruple Helix' model, bringing together government, business, academia, and civil society, could be constructive.

If the proposed National Centre for Critical Source Awareness is established, as outlined in the Ministry of Education's strategy from 2025, it could make a valuable contribution to addressing the broader challenge of disinformation. However, while fact checking and increasing media literacy is important, it might not fully resolve the issue. Nonetheless, a strategic hub that aligns efforts across sectors, gathers knowledge and coordinates national responses could offer advantages. Having a central Norwegian hub for coordinating efforts to raise awareness and counter negative impacts, without this hub engaging in fact checking itself, is also recommended by the NSM (NSM, 2023).

The lack of coordination is not only a national issue. The recent report from the European Centre of Excellence for Countering Hybrid Threats (Kalenský & Hanhijärvi, 2025) underscores the absence of established mechanisms for cooperation between governmental and non-governmental actors also at the European level. Consequentially, it notes that neither sector sees the full picture, making regular information exchange essential. Permanent cooperation mechanisms could unify otherwise fragmented perspectives; for example, a unit or agency entirely dedicated to detecting and/or countering disinformation, and, as suggested also by Vilmer (2021: 28), 'a cross-departmental network sharing information on a regular basis, all able to function irrespective of the political will of the moment'.

Importantly, any national efforts to limit the adverse effects of disinformation and hybrid threats must be grounded in knowledge. Understanding the evolving nature of disinformation, its mechanisms and its societal impact is crucial. If the state's primary responsibility is to safeguard the security of its citizens, it must possess both the expertise and institutional capacity to withstand, adjust and evolve in the face of influence operations, particularly those targeting Norway's democratic institutions. This includes the ability to situate such operations within a broader landscape of tools used to undermine national resilience. Sweden's establishment of the Psychological Defence Agency (MPF) offers a concrete example of how such a function can be institutionalized to protect democratic values and societal trust.

Freihse & Bochert (2024) suggest, based on their research, that a counter-disinformation agency should be placed under the office of the president or prime minister, precisely because disinformation is a topic that concerns many different political areas and ministries, which can easily lead to ministerial infighting over who is responsible. Some of the experts consulted referred to inter-ministerial cooperation as a 'daily struggle' (Freihse & Bochert, 2024). In Sweden, the MPF is mandated by the government to act as the principal *coordinator* for psychological defence. This means that it does not perform all the tasks itself, but has responsibility for how they are defined, conducted and organized. It is the hub within the government collecting expertise and capabilities on how psychological defence contributes to these areas, while other agencies have specialized roles within different parts of each area (Pamment & Isaksson, 2024: 8f). A similar function in Norway could improve situational awareness at the national level, which has been defined as

an essential step in building resilience. That such a unit would operate outside the Ministry of Defence, given its cross-sectoral remit and democratic focus, could help avoid conflating psychological defence with military strategy and thus strengthen its societal legitimacy. At the same time, if the MoD considers media literacy a strategic defence issue, it may be relevant to further formally integrate this aspect of resilience-building into national security and defence policy, to allow for cross-sector and longer-term capacity building in this field.

### 7.2.2. Recommendation 2: Contribute to improving conceptual clarity

Another emerging challenge is conceptual ambiguity, which better coordination could help solve. Terms like 'influence operations', 'information operations', 'psychological operations', 'misinformation' and 'disinformation' are often used interchangeably, despite having distinct meanings and scopes. Discussing terminology is not only of academic or linguistic value. The practical consequences of using unclear terms are that it can lead to threat assessments and analyses that cannot be applied across sectors and thus create poorer conditions for effective coordination and targeted measures (Bergersen, 2025). It can also lead to coordination gaps and misaligned policy responses (Caspari, 2021). Caspari concludes that, to confront a hybrid threat, the authorities must first establish a shared understanding of the problem, before they can develop a common situational awareness (Caspari, 2021). Actively engaging in international forums to clarify and standardize definitions seems relevant. As we have seen, the deliberate use of the term FIMI (Foreign Information Manipulation and Interference), which clearly delineates the scope of responsibility and reinforces that domestic citizens are not part of the threat picture beyond representing potential vulnerabilities, has contributed with an important distinction for the MPF in Sweden.

Furthermore, overusing the term 'warfare' can obscure these distinctions and hinder analytical clarity, unless referring to activities that clearly fall within a military framework. As described in Chapter 3.2, referring to disinformation or the information operations where it is encountered as forms of warfare can be said to impose a military framing on what might rather be political, social, or informational challenges. In theory, this framing may escalate tensions, justify exceptional measures like surveillance or censorship, and contribute to a blurring of the boundaries between civilian and military domains. A step towards mitigating these risks is to clarify definitions and to consider using more neutral terms unless referring to actual military contexts. Emphasizing the spectrum of activities involved, which might range from benign influence to hostile manipulation, can also help preserve conceptual precision and avoid unnecessary escalation. On the operational side, Vilmer (2021) similarly describes how an effective state response to disinformation should focus the ability to clearly define the threat: What are we talking about? Disinformation, information manipulation, information influence, foreign interference, or hybrid threats? (Vilmer, 2021: 28).

We thus echo the idea by Bergaust et al. (2022) who argue that a better understanding and a shared vocabulary is needed:

> To develop effective policies for addressing complex threats, researchers argue that we need a better understanding and a shared vocabulary. The term complex threats encompasses a wide range of events that vary in intensity and severity. Some disruptions must be tolerated, while others require active prevention and defence. *(Bergaust et al., 2022, own translation from Norwegian to English)*

They point to this as a difficult balancing act for authorities:

> […] we do not want a surveillance society, but we also cannot afford to be overly vulnerable. The challenge lies in implementing measures that do not compromise the very values we seek to protect. A sound and proportionate policy response depends on a clear and commonly accepted understanding of what constitutes a complex threat. *(Bergaust et al., 2022, own translation from Norwegian to English)*

Clarifying core concepts and terminology is not just a theoretical requirement, derived from research disciplines – it is equally critical in practice. As we have pointed to, developments in Sweden illustrate this, as we see how the MPF's concern about conceptual ambiguity underscores the need for far greater precision in how governments and institutions define, understand and respond to information threats. Concretely, as Pammant and Isaksson (2024) argue, the term *disinformation* has often been used too broadly, obscuring the distinct nature of the challenges at hand, both when it comes to everyday misinformation and coordinated influence operations and foreign interference. Recognizing these differences is considered essential for developing effective, targeted responses. Conceptual clarity also matters when it comes to assigning roles and responsibilities across sectors. From this, we propose that a focus on terms and concepts is not merely an academic or semantic exercise, but that it can be seen as foundational to building trust and democratic resilience.

### 7.2.3. Recommendation 3: Prioritize strategic and transparent communication

Based on what has been described in this PRIO Paper, there is reason to claim that public awareness and situational understanding of today's threat landscape could be further strengthened. Although the Armed Forces already carry out substantial communication efforts and the value of transparency is well recognized (Kvarving, 2025), there is an emerging need for more systematic and strategic engagement. Prioritizing strategic public communication will be essential in helping the population better understand disinformation and hybrid threats, in line with the recommendations set out in Norway's 2025 strategy against disinformation. This includes transparent messaging from both civil and military actors, reinforcing shared values such as press freedom.

If these values are not protected, the foundation of societal resilience is weakened. As the Freedom of Expression Commission's Report (NOU 2022:9) points out, safeguarding an open and enlightened public discourse requires more than legal protections, it demands a strong civil society and thoughtful communication strategies. The importance of a continuous focus on communicating with the public has been emphasized by the MPF, and it is acknowledged that this area requires further investment also in Sweden, especially due to the link between public knowledge and trust.

To build and maintain trust, knowledge about the person or entity you are meant to be trusting is necessary. It is hard to trust something or someone that you are not familiar with. This makes strategic communication aimed at raising awareness even more important. The 2025 Oscarsborg Symposium on Nordic Security (organized by PRIO) had as its point of departure the fact that security in the Nordic region is deteriorating rapidly due to rising geopolitical tensions. The Symposium addressed two critical communication challenges relevant for preparing the population to handle this new situation: first, how the Nordic countries conduct public communication to raise war risk awareness; and second, how they counter disinformation targeting Nordic cooperation and cohesion on defence and national security. Considering the various Nordic experiences on public war risk awareness communication campaigns, it was generally underlined as crucial to consider how variations in factors such as demographic heterogeneity and diversity, history, and geography, as well as the role of media, play into the formulation of information, awareness raising and debate.

As seen in the international survey by Kalenský and Hanhijärvi (2025: 12), less than half of the respondents evaluate their government's response to disinformation as well-communicated and transparent to the public. It is our understanding that a better explained, better communicated and more transparent policy has a better chance of gaining public trust. The communications unit of the MoD is tasked with developing and implementing communication strategies that support both political leadership and operational readiness, including crisis communication and digital outreach, and to coordinate strategic communication in the defence sector, as well as international defence cooperation. This report has not analysed or looked in particular at the strategic communication by the MoD, but we want to highlight the importance and continued relevance of investing in strategic communication, not only as a tool for crisis response, but as a long-term effort to build public trust and institutional credibility. In the Norwegian context, where transparency and democratic values are central, strategic communication plays a vital role in fostering confidence in the MoD and ensuring that its actions are understood and supported by the broader population.

*[A] better explained, better communicated and more transparent policy has a better chance of gaining public trust.*

Furthermore, in preparation for a potential situation where it is critical that information from the MoD reaches the public, strategic communication with a trust-building purpose is highly valuable. This emphasis is reflected in recent policy documents, including Meld. St. 33 (2024–2025), which highlights the need for improved situational awareness and public engagement in response to an increasingly complex threat landscape. Keeping the focus on how best to communicate (when, how, which channels, how much, etc.) is likely to contribute to increasing public knowledge and situational awareness related to disinformation and hybrid threats. This also adheres to the recommendations in the new national strategy for increasing resilience to disinformation (Ministry of Culture and Equality, 2025). The recommendation to communicate regularly about disinformation and the measures taken to counter it – for example by publishing national strategies, speeches, interviews and op-eds, including on social media platforms, both for awareness and deterrence purposes – is raised also by e.g. Vilmer (2021). This communication could take place via already existing channels.

The national risk assessments by the NSM, as well as the annual public threat assessments of both the PST and the NIS, are good examples of how to communicate about risks and threats in a transparent way. However, as suggested by Lif (2021), risks and threat scenarios highlighted in such reports could be communicated more broadly and consistently over time. By further developing, coordinating and strengthening national communication in these fields, the population can be better prepared for future crises, and potential information vacuums can be reduced. Sharing more information, also outside an actual crisis, can help build trust and create awareness of vulnerabilities. In this context, using the survey results presented in Chapter 6.2 as a backdrop, we suggest that it might be valuable to consider also where people tend to turn for information during a crisis, what the level of trust in different institutions are, where and how people read news, and what their social media behaviour generally is.

*Sharing more information, also outside an actual crisis, can help build trust and create awareness of vulnerabilities.*

### 7.2.4. Recommendation 4: Strengthen trust through public awareness

A consistent theme across past and current Norwegian initiatives, as described in Chapter 4.1, is the need to enhance *awareness*, whether it concerns source criticism, individual preparedness, or public understanding of the threat and risk landscape. Building a society that is resilient to disinformation is easier in a culture of security awareness, which in turn requires a foundational understanding of the risks we face. If these risks are not openly discussed, it becomes more difficult to mobilize public support for protective measures. By raising awareness, we reduce vulnerability. Similarly, Meld. St. 9 (2022–2023) highlights public awareness and trust as key factors in resisting disinformation and maintaining national security.

It is important to raise awareness across sectors and at multiple levels of society, which also relates to the recommendation to strengthen the coordination of national efforts. This includes integrating strategic communication into preparedness planning, but also fostering public dialogue about hybrid threats, and ensuring that awareness-raising efforts are grounded in democratic values and institutional trust. While not identical in scope, the *Barnevernet* case in Norway demonstrates that Norway is not immune to similar influence tactics as we saw during the 'LVU campaign' in Sweden. To effectively manage and counter influence campaigns such as these, more is required than merely fighting disinformation. Comprehensive confidence-building measures are needed, which should include direct interaction between citizens and state and municipal authorities. Initiatives facilitating direct engagement between local leaders – such as mayors and police chiefs – and the public in everyday settings can for example foster confidence and reduce vulnerability to manipulation. As part of these efforts, particular attention should be given to for example immigrant communities and marginalized groups.

*Comprehensive confidence-building measures are needed, which should include direct interaction between citizens and state and municipal authorities. Initiatives facilitating direct engagement between local leaders – such as mayors and police chiefs – and the public in everyday settings can for example foster confidence and reduce vulnerability to manipulation.*

Knowledge is key for both parties in an awareness-raising effort. More work is needed to get a proper overview of public knowledge and insights when it comes to matters of importance to resilience, for example to what extent the public reads and relates to annual threat- and risk-assessment reports. Solid and systematic knowledge about public perceptions and knowledge over time, not just sporadic data or information linked to a specific issue, could facilitate more targeted and tailored public communication. It can be difficult to assess whether public awareness information campaigns effectively educate citizens about the threat of disinformation. Difficulties aside, based on the SMS-campaign described in Chapter 6.2, there are some indications that awareness campaigns do have an effect. According to the survey, there was some evidence that respondents performed better at discerning true headlines from false ones after the educational campaign. The fact that other countries, such as Iceland, have observed Norway's 'Stop. Think. Check.' campaign and followed suit is further indication that it is an effort which might be worth pursuing. The campaign was distributed in six different languages to reach several minority groups in society.

Another step towards increased resilience is to produce (more) publicly available reports on relevant and associated topics. According to Kalenský and Hanhijärvi (2025), only a handful of Hybrid CoE's Participating States and Organisations (PSOs) publish such reports aimed at the general public. In Norway, authorities such as the PST, NIS and NSM possess valuable insights into disinformation threats and risks. As a way of raising awareness, their annual unclassified

risk and threat assessments should be shared more widely to support a common understanding across public institutions, the private sector, and the general population. Transparent communication about defence policies, NATO cooperation, military exercises etc. helps raise awareness and fill information gaps that disinformation might otherwise exploit. Such communication would have to be carefully calculated against increasing undue fears in the population. There is also a certain feedback loop between public awareness and trust, where high trust increases the effectiveness of awareness efforts, and people are more receptive to messages from trusted sources. Effective awareness, then, can strengthen trust by demonstrating transparency, competence and shared values. To build and maintain public trust, the MoD could support and coordinate targeted public awareness initiatives that explain the nature, tactics and objectives of disinformation. A high degree of trust and credibility is crucial for public authorities in several fields, but in particular for those dealing with risk and threats, and for those who have to rely on the public during crises. Fundamentally, an informed public is a more resilient public, and hence trust-building through awareness is considered to be a central pillar of efforts to increase societal resilience.

## 7.3. Conclusions and reflections

Building resilience is a way of reducing vulnerabilities, but the path toward robust societal resilience is neither linear nor uniform. While complexities, coordination challenges and public perceptions present obstacles, these can be counterbalanced by opportunities for strategic cooperation and alignment, knowledge consolidation and meaningful engagement with citizens. Recognizing and reflecting on these dynamics appears essential for designing policies and efforts that are both effective and sustainable.

In addition to the overarching recommendations presented above, which are interlinked and to some degree overlapping, we further encourage reflection that could deepen the understanding of the shifting disinformation dynamics. As we have seen, a common response to disinformation is fact-checking and media-literacy initiatives. However, as we have also seen, research suggests that individuals knowingly share false information to reinforce personal beliefs or provoke reactions (Buchanan, 2020), and that falsehoods often spread faster than verified facts (Vosoughi & Aral, 2018). This suggests that the solution is not only stronger institutions declaring what is true or not, but also a more nuanced understanding of the social and psychological mechanisms at play, and what the challenges truly are. The aim of this report is thus also to contribute to a broader understanding of resilience to disinformation.

As has also been discussed, the challenge is not only the spread of false information with harmful intent, but also the potential erosion of trust in true information, which could be seen in relation to changing media habits, social media sharing behaviour, etc. This raises critical questions worthy of future reflection:

- In terms of societal vulnerability, what part of the problem remains unsolved even when the truth is generally known by the national population?
- In terms of external interference, what is left of the threat if all claims are fact-checked?
- What if people do not trust true information?

We do not propose answers to these questions, but we want to point to their importance. Sweden's model offers valuable insights: psychological defence is framed as a civic responsibility, closely linked to national security and democratic stability. It goes beyond fact checking and emphasizes trust-building, mental preparedness and societal cohesion. Norway could benefit from further investigating ways of integrating psychological defence more deeply and explicitly into its total defence framework, positioning societal trust as a core component of resilience. Based on the insights presented in this report, this work could benefit from a focus on the strengthening of national coordination, improving conceptual clarity, a prioritization of strategic and transparent communication, and increasing trust and public awareness. ■

# Notes

1. Such as the report from FFI by Bergaust et al. (2022), which three years ago recommended that the Defence Commission should consider how a modern psychological defence could be organized in Norway.

2. The authors also want to thank Research Professor Sebastian Schutte and Doctoral Researcher Mathilde B. Mjelva for valuable insights in the first stage of the project, as well as Giovanni Dini for proofreading.

3. The definition is inspired by a brief paper written for Oxfam staff working to make development resilient. It describes resilience capacity and what it looks like in practice (Jeans, Castillo & Thomas, 2017).

4. The following description is more or less cited (albeit shortened) from page 23 of the report.

5. The full list can be found in Kalenský & Hanhijärvi (2025: 8).

6. This paragraph is cited from page 41 of the report by NATO Strategic Communications Centre of Excellence (2026).

7. Based on information from a meeting at PRIO with General Major Oleksii Migrin, Deputy Head of SESU (State Emergency Service Ukraine), C Viktor Vitovetskyi, Director of the Civil Protection Department, Serhii Kravchenko, Senior Lieutenant of the International Cooperation Department at SESU (translator).

8. These numbers only show the first three years of the MPF being operational. The lack of data from 2025–2026 is because these were not yet available at the time this report was first submitted.

9. Förordning (2021:936) med instruktion för Myndigheten för psykologiskt försvar.

10. In Swedish: En ny myndighet för att stärka det psykologiska försvaret.

11. In Swedish: Lag med särskilda bestämmelser om vård av unga.

12. By the end of 2022, all 30 NATO states except Türkiye and Hungary had ratified Sweden's accession protocol. When it became clear in March 2023 that Finland would enter into NATO alone as its 31st member state, the Finnish Parliament also held a vote to ratify Sweden's accession protocol, again leaving only Türkiye and Hungary as the final two holdouts.

13. In February 2023, according to Hayward (2025), the overview for the same search was the following: 'combat disinformation' yielded 1,520 entries; this contrasted with 388 for 'identify disinformation', 154 for 'expose disinformation' and 38 for 'analyse disinformation'.

14. The survey presented here was funded and carried out in the context of the project 'Disinformation and people: impacts on societal trust and resilience (FAKENEWS)'. The project is led by Professor Gunhild Hoogensen Gjørv at the University of Tromsø. Senior Researcher Stine Bergersen, main author of the current report, led PRIO's part in the project. The survey was carried out by Norstat in Norway (by Gjørv, UiT and Bergersen, PRIO) and in Sweden (by Jannie Lilja and Ester Tottie, SIPRI and Niklas Eklund, University of Umeå). Several other project members contributed in different ways to the development of the surveys. The FAKENEWS project is funded by the Research Council of Norway and runs until August 2026.

Permission to use the data presented in Chapter 6.2 of this report has been acquired from the project leader. Furthermore, the project 'The Neglected Key to Defence' (funded by the Norwegian MoD), also led by Gjørv, provided the basis for the surveys for FAKENEWS. The SMS- intervention was based on the '*Stopp, tenk, sjekk*' campaign, launched by the Norwegian Media Authority in 2021.

15. Direktoratet for samfunnssikkerhet og beredskap (Norwegian Directorate for Civil Protection); Folkehelseinstituttet (Norwegian Institute of Public Health).

16. Some of the answers had to be shortened for the legibility of the graph; the second answer category was 'Police and emergency services', the third category was 'DSB, FHI or other national authorities' and the sixth category was 'Other Norwegian Radio & TV-channels'.

17. In the group of respondents who had only completed primary school, this number was 82%, but it is worth noting this group is significantly smaller than all the others, with only 80 respondents.

18. Note that respondents were asked separately about each 'entity' shown in Figure 5 and asked to rate them on a 7-point scale from least responsible to most responsible for countering disinformation – hence why the percentages add up to much more than 100%.

19. Like in Figure 3, here some of the answer categories had to be shortened for legibility; the first category was 'Traditional media such as newspapers, radio and TV', the fourth was 'Schools and educational institutions', and the sixth 'Social media platforms, such as X/Twitter, Facebook, Instagram etc.'.

20. Elzbieta Drazkiewicz works at Lund University and specializes in conspiracy theories, a phenomenon within disinformation. She also leads the Nordic Disinformation Resilience Network, funded by NordForsk, with scholars from social sciences and humanities.

# References


Aarli-Grøndalen, Roger (2024) Kildekritikk for første gang en del av egenberedskapen. *Journalisten*, 2 November. Available at: www.journalisten.no/notice/626476.

Ahlerup, Linda & Magnus Ranstorp (2023) *LVU-kampanjen: Desinformation, konspirationsteorier och kopplingarna mellan det inhemska och det internationella i relation till informationspåverkan från icke-statliga aktörer.* [*The LVU campaign: Disinformation, conspiracy theories and the connections between the domestic and the international in relation to information influence from non-state actors*]. Försvarshögskolan, Centrum för totalförsvar och samhällets säkerhet. Available at: www.fhs.se/download/18.32d29dd2187bd01d5e455265/1682576119173/LVU-kampanjen.pdf.

Aïmeur, Esma; Sabrine Amri & Gilles Brassard (2023) Fake news, disinformation and misinformation in social media: a review. *Social Network Analysis and Mining 13*, 30. DOI: 10.1007/s13278-023-01028-5.

Allcott, Hunt & Matthew Gentzkow (2017) Social Media and Fake News in the 2016 Election. *The Journal of Economic Perspectives* 31(2): 211–235. DOI: 10.1257/jep.31.2.211.

Bergaust, Julie Celine; Frida Skjei & Stig Rune Sellevåg (2022) *Hva kan Norge lære av andre lands tilnærming til sammensatte trusler? – rapport til Forsvarskommisjonen.* [*What can Norway learn from other countries' approaches to complex threats? – report to the Defence Commission*]. Rapport 22/02310. Forsvarets Forskningsinstitutt.

Bergersen, Stine (2025) Why we should stop talking about "fake news". *PRIO Comment*, 21 November. Available at: www.prio.org/comments/1835.

Berggreen Kaalaas, Sunniva (2025) Krigsfrykten har økt. [Fear of war has increased]. *Forsvarets forum*, 22 February. Available at: www.forsvaretsforum.no/krig-meningsmaling-norge/krigsfrykten-har-okt/424159.

Broda, Elena & Jesper Strömbäck (2024) Misinformation, disinformation, and fake news: lessons from an interdisciplinary, systematic literature review. *Annals of the International Communication Association* 48(2): 139–166. DOI: 10.1080/23808985.2024.2323736.

Buchanan, Tom (2020) Why do people spread false information online? The effects of message and viewer characteristics on self-reported likelihood of sharing social media disinformation. *PloS One* 15(10), e0239666. DOI: 10.1371/journal.pone.0239666.

Cabrera Blázquez, Francisco Javier; Maja Capello, Julio Talavera Milla & Sophie Valais (2022) *User empowerment against disinformation online.* European Audiovisual Observatory. Available at: rm.coe.int/iris-plus-2022en3-user-empowerment-against-disinformation/1680a963c4.

Carvin, Andy; Ksenia Iliuk & Roman Osadchuk (2023) Mapping the last decade of Russia's disinformation and influence campaign in Ukraine. *Atlantic Council*, 8 June. [Transcript]. Available at: www.atlanticcouncil.org/news/transcripts/mapping-the-last-decade-of-russias-disinformation-and-influence-campaign-in-ukraine.

Caspari, Bernhard (2021) *Norges forståelse av hybride trusler: Effektene av ulike konseptualiseringer på myndighetenes samarbeid* [*Norway's understanding of hybrid threats: The effects of different conceptualizations on government cooperation*]. Masteroppgave. Universitetet i Stavanger.

Catena, Beatrice; Ditrych, Ondrej & Nad'a Kovalčíková (2025) *Smoke and mirrors: building EU resilience against manipulation through cognitive security.* European Union Institute for Security Studies. Available at: data.europa.eu/doi/10.2815/8072408.

Coady, D. (2021) The Fake News about Fake News. In: Sven Bernecker; Amy K. Flowerree & Thomas Grundmann (eds) *The Epistemology of Fake News.* Oxford: Oxford University Press, 68–81. DOI: 10.1093/oso/9780198863977.003.0004.

Cohen, Raphael S.; Nathan Beauchamp-Mustafaga, Joe Cheravitch, Alyssa Demus, Scott W. Harold, Jeffrey W. Hornung, Jenny Jun, Michael Schwille, Elina Treyger & Nathan Vest (2021) *Combating Foreign Disinformation on Social Media: Study Overview and Conclusions.* RAND research report. RAND Corporation. Available at: www.rand.org/content/dam/rand/pubs/research_reports/RR4300/RR4373z1/RAND_RR4373z1.pdf.

Dame Adjin-Tettey, Theodora (2022) Combating fake news, disinformation, and misinformation: Experimental evidence for media literacy education. *Cogent Arts & Humanities* 9(1). DOI: 10.1080/23311983.2022.2037229.

D'Andrea, Alessia; Giorgia Fusacchia & Arianna D'Ulizia (2025) Policy Review: Countering Disinformation in the Digital Age – Policies and Initiatives to Safeguard Democracy in Europe. *Information Polity* 30(1): 82–91. DOI: 10.1177/15701255251318900.

The Digital Forensic Research Lab (2024) *Undermining Ukraine: How Russia widened its global information war in 2023.* Atlantic Council Report, 29 February. Available at: www.atlanticcouncil.org/in-depth-research-reports/report/undermining-ukraine-how-russia-widened-its-global-information-war-in-2023.

DISA Press Room (2025) Combating Disinformation Through Education and Technology: A Case Study of Finland. *Disinformation Social Media Alliance*, 21 March. Available at : disa.org/combating-disinformation-through-education-and-technology-a-case-study-of-finland.

Elsner, Mark; Grace Atkinson & Saadia Zahidi (2025) *Global Risks Report 2025.* World Economic Forum. Available at: www.weforum.org/publications/global-risks-report-2025.

European Commission (2018) *Action Plan against Disinformation.* Available at: commission.europa.eu/publications/action-plan-disinformation-commission-contribution-european-council-13-14-december-2018_en.

European Commission (2020) *The EU's Cybersecurity Strategy for the Digital Decade.* Available at: eur-lex.europa.eu/legal-content/EN/TXT/?uri=JOIN%3A2020%3A18%3AFIN.

EU Disinfo Lab (2023) *FIMI: Towards a European Redefinition of Foreign Interference.* www.disinfo.eu/wp-content/uploads/2023/04/20230412_FIMI-FS-FINAL.pdf.

Filipec, Ondrej (2019) Towards a disinformation resilient society? The experience of the Czech Republic. *Cosmopolitan Civil Societies* 11(1): 1–26. DOI: 10.5130/ccs.v11.i1.6065.

Freihse, Charlotte & Florian Bochert (2024) Up to the challenge? Strategies to counter disinformation in the EU, UK and US. *Upgrade Democracy.* Bertelsmann Stiftung, Gütersloh. DOI: 10.11586/2024161.

Gjeseth, Gullow (2016) *Forsvarskommisjonen av 1946. Planleggingen av norsk etterkrigsforsvar på 1940-tallet.*

[*The Defense Commission of 1946. The planning of Norwegian post-war defence in the 1940s*]. Institutt for forsvarsstudier.

Goodman, Emma (2021) *Media literacy in Europe and the role of EDMO.* European Digital Media Observatory. Available at: edmo.eu/wp-content/uploads/2022/02/Media-literacy-in-Europe-and-the-role-of-EDMO-Report-2021.pdf.

Grahn, Hikka & Toni Taipalus (2025) Defining comprehensive cognitive security in the digital era: Literature review and concept analysis. *Journal of Information Warfare* 24(2): 39–59. Available at: www.jinfowar.com/journal/volume-24-issue-2/defining-comprehensive-cognitive-security-digital-era-literature-review-concept-analysis.

Guess, Andrew M. & Lyons, Benjamin A. (2020) Misinformation, Disinformation, and Online Propaganda. In: Nathaniel Persily & Joshua A. Tucker (eds) *Social Media and Democracy.* Cambridge: Cambridge University Press, 10–33.

Habgood-Coote, Joshua (2018) Stop talking about fake news! *Inquiry* 62(9–10): 1033–1065. DOI: 10.1080/0020174X.2018.1508363.

Handler, Simon (2023) Conflict in Ukraine's information environment. *The 5x5*, 22 March. Cyber Statecraft Initiative, Atlantic Council. Available at: www.atlanticcouncil.org/content-series/the-5x5/the-5x5-conflict-in-ukraines-information-environment.

Hayward, Tim (2025) The Problem of Disinformation: A Critical Approach. *Social Epistemology 39*(1): 1–23. DOI: 10.1080/02691728.2024.2346127.

Humprecht, Edda; Frank Esser & Peter Van Aelst (2020) Resilience to Online Disinformation: A Framework for Cross-National Comparative Research. *The International Journal of Press/Politics* 25(3): 493–516. DOI: 10.1177/1940161219900126.

Ibrahim, Fabio; Steffen Rhode & Monika Dasek-ing (2023) A Systematic Review of Cognitive and Psychological Warfare. *The Defence Horizon Journal Blog.* Available at: tdhj.org/blog/post/cognitive-psychological-warfare.

Innst. 392 S (2021–2022). Innstilling fra utenriks- og forsvarskomiteen om Prioriterte endringer, status og tiltak i forsvarssektoren. [Recommendation from the Foreign Affairs and Defence Committee on Priority Changes, Status and Measures in the Defence Sector]. Available at: www.stortinget.no/no/Saker-og-publikasjoner/Publikasjoner/Innstillinger/Stortinget/2021-2022/inns-202122-392s/?all=true.

Innst. 247 S (2022–2023) Innstilling fra justiskomiteen om Nasjonal kontroll og digital motstandskraft for å ivareta nasjonal sikkerhet. [Recommendation from the Judiciary Committee on National Control and Digital Resilience to Ensure National Security]. Available at: www.stortinget.no/no/Saker-og-publikasjoner/Publikasjoner/Innstillinger/Stortinget/2022-2023/inns-202223-247s/?all=true.

Jeans, Helen; Gina E. Castillo, Sebastian Thomas (2017) Absorb, Adapt, Transform: Resilience capacities. *Oxfam Policy and Practice*, 25 January. Available at: policy-practice.oxfam.org/resources/absorb-adapt-transform-resilience-capacities-620178.

Kalenský, Jakub (2022) How to Defend Against Covid Related Disinformation. In: Ritu Gill & Rebecca Goolsby (eds) *COVID-19 Disinformation: A Multi-National, Whole of Society Perspective.* Advanced Sciences and Technologies for Security Applications. Springer, Cham. DOI: 10.1007/978-3-030-94825-2_7.

Kalenský, Jakub & Heidi Hanhijärvi (2025) *Countering disinformation in the Euro-Atlantic: Strengths and gaps.* European Centre of Excellence for Countering Hybrid Threats. Available at: www.hybridcoe.fi/wp-content/uploads/2025/10/Hybrid_CoE_Research_Report_15_Countering_disinformation_Euro_Atlantic.pdf.

Kapantai, Eleni; Androniki Christopoulou, Christos Berberidis & Vassilios Peristeras (2021) A systematic literature review on disinformation: Toward a unified taxonomical framework. *New Media & Society* 23(5): 1301–1326. DOI: 10.1177/1461444820959296.

Kozłowski, Andrzej (2024) Combatting disinformation by state agencies: the case of the Swedish Psychological Defence Agency. *New Eastern Europe.* Available at: neweasterneurope.eu/2024/05/07/combatting-disinformation-by-state-agencies-the-case-of-the-swedish-psychological-defence-agency.

Kvarving, Eystein (2025) I forsvaret skal vi være åpne og ærlige. [In the Armed forces we will be open and honest]. *Aftenposten* Kronikk, 17 November. Available at: www.aftenposten.no/meninger/debatt/i/xmxa0j/i-forsvaret-skal-vi-vaere-aapne-og-aerlige.

Lazer, David M. J.; Matthew A. Baum, Yochai Benkler, Adam J. Berinsky, Kelly M. Greenhill, Filippo Menczer, Miriam J. Metzger, Brendan Nyhan, Gordon Pennycook, David Rothschild, Michael Schudson, Steven A. Sloman, Cass R. Sunstein, Emily A. Thorson, Duncan J. Watts & Jonathan L. Zittrain (2018) The science of fake news. *Science (American Association for the Advancement of Science)* 359(6380): 1094–1096. DOI: 10.1126/science.aao2998.

Le Guyader, Hervé (2022) Cognitive domain: A sixth domain of operations. In: Bernard Claverie; Baptiste Prébot, Norbou Buchler & François du Cluzel (eds) *Cognitive warfare: The future of cognitive dominance.* NATO Collaboration Support Office, 3–5. Available at: hal.science/hal-03635898/document.

Lif, Anton (2021) Nordisk samarbeid for psykologisk forsvar: 10 forslag. [Nordic cooperation for psychological defence: 10 suggestions]. *Utsyn – Senter for sikkerhet og totalforsvar.* Available at: www.prosjektutsyn.no/nordisk-samarbeid-for-psykologisk-forsvar-10-forslag.

Lif, Anton (2024) Sverige under press. [Sweden under pressure]. *Utsyn – Senter for sikkerhet og totalforsvar.* Available at: www.prosjektutsyn.no/sverige-under-press.

Lindgren, Johannes; James Pamment, Angela Palmer, Sanda Svetoka & Elīna Lange-Ionatamišvili (2026) Countering Information Influence Operations in the Nordic-Baltic Region. NATO Strategic Communications Centre of Excellence. Available at: stratcomcoe.org/pdfjs/?file=/publications/download/Countering-IIOs-in-the-Nordic-Baltic-FINAL-FILE.pdf?zoom=page-fit.

Meld. St. 5 (2020–2021) *Samfunnssikkerhet i en usikker verden.* [Societal security in an uncertain world]. Norwegian Ministry of Justice and Public Security. Available at: www.regjeringen.no/no/dokumenter/meld.-st.-5-20202021/id2770928.

Meld. St. 9 (2022–2023) *Nasjonal kontroll og digital motstandskraft for å ivareta nasjonal sikkerhet – Så åpent som mulig, så sikkert som nødvendig.* [National control and digital resilience to safeguard national security – as open as possible, as secure as necessary]. Norwegian Ministry of Justice and Public Security. Available at: www.regjeringen.no/no/dokumenter/meld.-st.-9-20222023/id2950130/?ch=3.

Meld. St. 10 (2021–2022) *Prioriterte endringer, status og tiltak i forsvarssektoren.* [Priority changes, status, and measures in the defence sector]. Norwegian Ministry of Defense. Available at: www.regjeringen.no/no/dokumenter/meld.-st.-10-20212022/id2908167.

MPF (2023) *Struktur för effektiv samverkan för det psykologiska försvaret - Slutredovisning av regeringens uppdrag till Myndigheten för psykologiskt försvar (Ju2021/04162).* [Framework for effective coordination for psychological defence – Final report on the government's mandate to the Swedish Agency for Psychological Defence]. Swedish Psychological Defense Agency. MPF/2023:56. Available at: mpf.se/download/18.660bf8cf18c8acbdb7930b94/1704207823333/struktur-for-effektiv-samverkan--for-det-psykologiska-forsvaret-slutredovisning.pdf.

MPF (2025) *Opinioner 2024 - Allmänhetens syn på samhällsskydd, beredskap, säkerhetspolitik och försvar.* [*Public Opinion 2024 – The public's views on societal protection, preparedness, security policy, and defence*]. Swedish Psychological Defense Agency. Available at: mpf.se/publikationer/publikationer/2025-01-15-opinioner-2024.

NATO (2016) *Commitment to enhance resilience.* North Atlantic Treaty Organization, 8 July. Available at: www.nato.int/en/about-us/official-texts-and-resources/official-texts/2016/07/08/commitment-to-enhance-resilience.

NATO (1949) *North Atlantic Treaty.* North Atlantic Treaty Organization. Available at: www.nato.int/en/about-us/official-texts-and-resources/official-texts/1949/04/04/the-north-atlantic-treaty.

NATO (n.d.) *Cognitive Warfare.* North Atlantic Treaty Organization. Available at: www.act.nato.int/activities/cognitive-warfare.

NIS (2024) *Focus 2024 - The Norwegian Intelligence Service's assessment of current security challenges.* Norwegian Intelligence Service. Available at: www.etterretningstjenesten.no/publikasjoner/focus/Focus24_contents.

NordForsk. (2025) *Disinformation is now part of mainstream politics.* NordForsk. Available at: www.nordforsk.org/news/disinformation-now-part-mainstream-politics.

NOU 2022:9 (2022) *En åpen og opplyst offentlig samtale.* [*An open and informed public discourse*]. Ytringsfrihetskommisjonen. Available at: www.regjeringen.no/no/dokumenter/nou-2022-9/id2924020.

NOU 2023:17 (2023) *Nå er det alvor – Rustet for en usikker fremtid.* [*Now it's Serious – Prepared for an uncertain future*]. Totalberedskapskommisjonen. Available at: www.regjeringen.no/no/dokumenter/nou-2023-17/id2982767.

NSM (2023) Sikkerhetsfaglig råd - Et motstandsdyktig Norge. [Security Advisory Council – A Resilient Norway]. Najonal Sikkerhetsmyndighet. Available at: nsm.no/getfile.php/1312994-1683615611/NSM/Filer/Dokumenter/Rapporter/Sikkerhetsfaglig%20r%C3%A5d%20-%20Et%20motstandsdyktig%20Norge.pdf.

Office of the Norwegian Prime Minister (2025) *National Security Strategy.* Available at: www.regjeringen.no/en/documents/national-security-strategy/id3099304/?ch=1.

Ördén, Hedvig (2025) A genealogy of Swedish psychological defence: Information influence as a shifting problem for democratic governance. *Cooperation and Conflict* 60(4): 1005–1027. DOI: 10.1177/00108367251336980.

Palfrey, John (2025) *Misinformation and disinformation.* Encyclopaedia Britannica. Available at: www.britannica.com/topic/misinformation-and-disinformation.

Palmertz, Björn; Mikael Weissmann, Niklas Nilsson & Johan Engvall (2024) *Building Resilience and Psychological Defence – An analytical framework for countering hybrid threats and foreign influence and interference.* Lund University. Psychological Defence Research Institute. Working Paper 2024:1. Available at: www.psychologicaldefence.lu.se/sites/psychologicaldefence.lu.se/files/2024-03/BuidlingResilienceAndPsychologicalDefence.pdf.

Pamment, James & Elsa Isaksson (2024) *Psychological Defence: Concepts and principles for the 2020s.* Lund University. Psychological Defence Research Institute. MPF Report Series 6/2024. Available at: mpf.se/psychological-defence-agency/publications/archive/2024-10-28-psychological-defence-concepts-and-principles-for-the-2020s.

Pennycook, Gordon; Ziv Epstein, Mohsen Mosleh, Antonio A. Arechar, Dean Eckles & David G. Rand (2021) Shifting attention to accuracy can reduce misinformation online. *Nature* 592(7855): 590–595. DOI: 10.1038/s41586-021-03344-2.

Prop. 14 S (2020–2021) *Evne til forsvar – vilje til beredskap Langtidsplan for forsvarssektoren.* [*Capability to Defend – Willingness for preparedness. The Long-Term Plan for the Defence Sector*]. Norwegian Ministry of Defense. Available at: www.regjeringen.no/no/dokumenter/prop.-14-s-20202021/id2770783.

Psykologtidningen (2022) Psykologimyndigheten nobbar psykologer. [The Psychological Authority rejects psychologists]. *Psykologtidningen*. Available at: psykologtidningen.se/2022/04/25/psykologimyndigheten-nobbar-psykologer.

RAND (2025) Information Operations. Available at: www.rand.org/topics/information-operations.html.

Riksrevisjonen (2025) *Totalforsvaret i sikkerhetspolitisk krise og krig* (Dokument 3:11 (2024–2025)). [The Total Defence in a Security-Policy Crisis and War]. Riksrevisjonen. Available at: www.riksrevisjonen.no/rapporter-mappe/no-2024-2025/totalforsvaret-i-sikkerhetspolitisk-krise-og-krig.

Roozenbeek, Jon & Sander van der Linden (2019) Fake news game confers psychological resistance against online misinformation. *Humanities & Social Sciences Communications* 5(65). DOI: 10.1057/s41599-019-0279-9.

Samuelsen, Reidun J. (2023) Farlige ord: De hemmelige tjenestenes forståelse av desinformasjon som en samfunnstrussel. [Dangerous words: How the Intelligence Services understand disinformation as a societal threat]. *Norsk Medietidsskrift* 30(2): 1–16. DOI: 10.18261/nmt.30.2.3.

The Security Committee (2017) *The Security Strategy for Society.* Government Resolution 2.11.2017. Available at: turvallisuuskomitea.fi/wp-content/uploads/2018/04/YTS_2017_english.pdf.

SFS 2021:936 (2021) *Förordning (2021:936) med instruktion för Myndigheten för psykologiskt försvar.* [*Ordinance (2021:936) containing instructions for the Swedish Agency for Psychological Defence*]. Swedish Ministry of Defense. Available at: www.riksdagen.se/sv/dokument-och-lagar/dokument/svensk-forfattningssamling/forordning-2021936-med-instruktion-for_sfs-2021-936.

Sivertsen, Eskil G.; Nina Hellum, Arild Bergh & Anna L. Bjørnstad (2021) *Hvordan gjøre samfunnet mer robust mot uønsket påvirkning i sosiale medier.*

Rapport 21/01237. [*How to make society more resilient to unwanted influence on social media*]. Forsvarets Forskningsinstitutt. Available at: www.ffi.no/publikasjoner/arkiv/hvordan-gjore-samfunnet-mer-robust-mot-uonsket-pavirkning-i-sosiale-medier.

Sivertsen, Eskil G. (2024) FFI-forsker til næringslivseliten: – Vi gjør sørgelig lite for å svare på russisk påvirkning. [FFI researcher to the business elite: "We are doing far too little to respond to Russian influence"]. *Forskning.no.* Available at: www.forskning.no/forsvaret-krig-ntb/ffi-forsker-til-naeringslivseliten-vi-gjor-sorgelig-lite-for-a-svare-pa-russisk-pavirkning/2307338.

SOU 2020:29 (2020) *En ny myndighet för att stärka det psykologiska försvaret.* [A new authority to strengthen psychological defence]. Swedish Ministry of Justice. Available at: www.regeringen.se/rattsliga-dokument/statens-offentliga-utredningar/2020/05/sou-202029.

SPRAVDI (2025) The School for Strategic Communications and Information Security. *Ukrainian Centre for Strategic Communication.* Available at: spravdi.gov.ua/en/school-of-countering-disinformation.

Strategi for å styrkje motstandskrafta mot desinformasjon (2025–2030) [Strategy for strengthening resilience against disinformation (2025-2030)] (2025) Ministry of Culture and Equality. Available at: www.regjeringen.no/no/dokumenter/strategi-for-a-styrkje-motstandskrafta-mot-desinformasjon-2025-2030/id3109255.

Suliman, Adela (2022) Sweden sets up Psychological Defense Agency to fight fake news, foreign interference. *The Washington Post.* Available at: www.washingtonpost.com/world/2022/01/06/sweden-fake-news-psychological-defence-agency.

Sundby Fallmyr, Synnøve; Emilie Waaler & Hilde Nilsson Ridola (2025) Ny rapport: Forsvaret mangler penger, folk og utstyr. [New report: The armed forces are missing funding, people and equipment]. *NRK*, 18 February. Available at: www.nrk.no/norge/ny-rapport-fra-forsvarets-forskningsinstitutt_-norsk-forsvar-mangler-penger_-folk-og-utstyr-1.17289140.

Tandoc, Edson C.; Darren Lim & Rich Ling (2020) Diffusion of disinformation: How social media users respond to fake news and why. *Journalism* 21(3): 381–398. DOI: 10.1177/1464884919868325.

Vignium (2022) Service de vigilance et protection contre les ingérences numériques étrangères. [Service for vigilance and protection against foreign digital interference]. Available at: www.sgdsn.gouv.fr/notre-organisation/composantes/service-de-vigilance-et-protection-contre-les-ingerences-numeriques.

Vilmer, Jean-Baptiste Jeangène (2021) *Effective state practices against disinformation: Four country case studies.* European Centre of Excellence for Countering Hybrid Threats. Available at: www.hybridcoe.fi/wp-content/uploads/2021/07/20210709_Hybrid_CoE_Research_Report_2_Effective_state_practices_against_disinformation_WEB.pdf.

Vosoughi, Soroush; Deb Roy & Sinan Aral (2018) The spread of true and false news online. *Science (American Association for the Advancement of Science)* 359(6380): 1146–1151. DOI: 10.1126/science.aap9559.

Wardle, Claire & Hossein Derakhshan (2017) *Information Disorder: Toward an interdisciplinary framework for research and policy making.* Council of Europe Report, DGI (2017)09. Available at: edoc.coe.int/en/media/7495-information-disorder-toward-an-interdisciplinary-framework-for-research-and-policy-making.html.

World Economic Forum (2026) The Global Risks Report 2026. 21st Edition. Insight report. Available at: reports.weforum.org/docs/WEF_Global_Risks_Report_2026.pdf

Wigell, Mikael (2021) Democratic Deterrence: How to Dissuade Hybrid Interference. *The Washington Quarterly* 44(1): 49–67. DOI: 10.1080/0163660X.2021.1893027.

Wither, James Kenneth (2020) Back to the future? Nordic total defence concepts. *Defence Studies* 20(1): 61–81. DOI: 10.1080/14702436.2020.1718498.

# Increasing resilience in the age of disinformation

*Recommendations for enhanced preparedness through collective psychological defence*

Disinformation poses a growing threat to democratic societies by undermining trust in public institutions and weakening democratic resilience. The World Economic Forum ranked misinformation and disinformation as the top global risk in 2025 and the second most severe in 2026. This PRIO Paper highlights some important aspects to consider when addressing these challenges with reference to the concept of psychological defence. Psychological defence emphasizes societal resilience against hybrid threats such as disinformation rather than solely countering false claims. Drawing on European experiences and the Norwegian context, the report concludes that a whole-of-society approach is essential. Traditional measures like fact checking and media literacy remain important but are insufficient on their own, as disinformation often targets trust rather than accuracy. Strong national coordination, clear terminology, strategic communication and sustained trust-building, also outside crisis situations, are highlighted as critical. Ultimately, strengthening psychological defence can help safeguard democratic values and public confidence in an increasingly complex security environment.

Stine Bergersen
*Peace Research Institute Oslo (PRIO)*

Gabriel Lönn
*Peace Research Institute Oslo (PRIO)*

PRIO