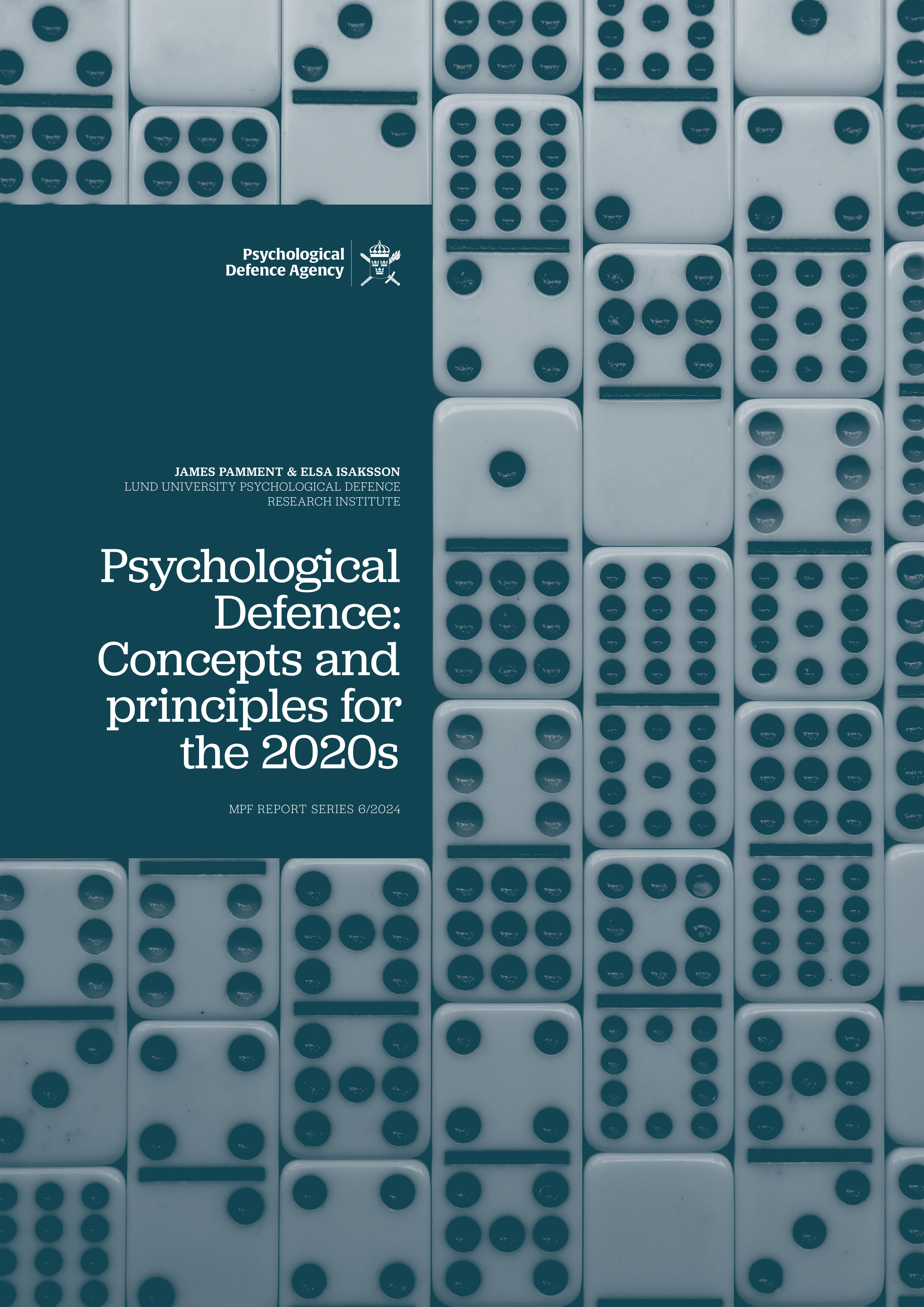


Psychological
Defence Agency

JAMES PAMMENT & ELSA ISAKSSON
LUND UNIVERSITY PSYCHOLOGICAL DEFENCE
RESEARCH INSTITUTE

Psychological Defence: Concepts and principles for the 2020s

MPF REPORT SERIES 6/2024

Contents

PSYCHOLOGICAL DEFENCE: CONCEPTS AND PRINCIPLES FOR THE 2020S
© Myndigheten för psykologiskt försvar (MPF)
Photo: Mick Haupt/Unsplash
Print: Scandinavian Print Group AB
Production: Kid id
ISBN: 978-91-989646-0-8

Foreword

Foreign information manipulation and interference (FIMI) is not a new phenomenon. Since the end of the Second World War, when Sweden seriously began to work with psychological defense to respond to various forms of hybrid threats, the issue has been prevalent and developing. This groundwork report not just portraits the evolution of Sweden's psychological defence from the 1950s to its accentuated relevance in today's era, the authors also highlight how modern psychological defence differs from previous forms. While there are clear connections to the historical approach, essential differences such as threats in the digital domain and the importance of increased international cooperation are emphasized.

The reports main contribution, however, concerns outlining how the concept of psychological defence has developed over the years, where it stands today, and not least future challenges. This is an area that has needed development in recent years, not just for its own sake but also because it provides a base and a structure for future development. The authors presentation of psychological defence in the form of four principles (resilience, threat intelligence, deterrence, and strategic communication) constitutes a promising theoretical contribution to the field, and perhaps also the foundation for a practical framework.

The report brings to attention the central role of external threats actors in modern psychological defense, not just as a driving force but also concerning how counteractions could be designed and implemented. This focus is based on an understanding of the specific threats that Sweden faces, as well as knowing our own vulnerabilities. By continuously analyzing and understanding such threats, combined with strengthening the populations resilience and will-to-fight, Sweden can better prepare for, and meet, the challenges posed by FIMI and hybrid threats.

For a good number of years, democracy as a form of governance has been pushed back globally and autocracies have not just gained ground, but also become more bolden and less risk-averse. This is also the case regarding FIMI, not least since autocracies tend to get away with lying and manipulate public opinion on the one hand, whereas political accountability and independent media are more or less non-existent on the other. The information arena is a looming challenge for Sweden and our friends and allies in the years ahead – and this timely report brings structure to a rapidly evolving field.

This report is part of the multi-year support the Swedish Psychological Defence Agency provides to the Psychological Defence Research Institute at Lund University.

The authors are responsible for the content and conclusions of the report.

Magnus Hjort
Director General

1 | Introduction

1. Introduction

“The purpose of psychological defence is to safeguard our open and democratic society, the free formation of opinion, Sweden’s fundamental freedoms and ultimately our independence. The psychological defence identifies, analyses, prevents, and counters foreign malign information influence activities and other disinformation directed at Sweden or at Swedish interests. This could include attempts from foreign actors to weaken national resilience and the population’s will to defend the country, or malign influence aimed at changing people’s perceptions or influencing behaviours and the decision-making in society.”

– The Swedish Psychological Defence Agency, 2022

Since the launch of the Swedish Psychological Defence Agency (*Myndigheten för psykologiskt försvar*, MPF) in January 2022, there has been a great deal of interest in what psychological defence means in its modern interpretation. Indeed, from the moment of its inception, the reaction of some has been to ask why other countries do not have a public agency with a similar role (Braw 2022). Furthermore, in May 2024, President of the European Commission Ursula von der Leyen suggested the need for a European-level agency performing an equivalent function to MPF (von der Leyen 2024). Yet, the announcement of the new agency by former PM Stefan Löfven back in January 2018 was somewhat unexpected, since he placed upon the new agency the baggage of a Cold War terminology, and potentially an outdated function.

As a term that came to the fore in Sweden during the 1950s, psychological defence is loaded with connotations. In Freudian psychology, it refers to the unconscious methods by which we protect ourselves from anxiety, *psychological defence mechanisms* (Bailey & Pico 2022). Its political appropriation in Sweden saw the term used within the concept of total defence to describe the resilience of a country to foreign propaganda. When adversaries conduct *psychological warfare*, Sweden needs a *psychological defence*. Although its focus evolved over the years, in essence the concept covered protection of democratic foundations such as freedom of speech and the media system, safeguarding of the will to defend, analysis of foreign propaganda efforts, and an ability to counteract hostile influence both domestically and abroad if necessary (Rossbach 2017).

Since the Psychological Defence Board had its mandate significantly reduced in 2002 before finally being disbanded in 2008, much has changed in geopolitics, technology, and information consumption. This is reflected in a policy area which now uses terms such as disinformation, influence operations, information manipulation, FIMI[1], hybrid threats, and foreign interference. What, then, is the value of a concept such as psychological defence in the 2020s? What does it offer to an already overloaded terminological apparatus beyond yet another poorly defined concept to use? And how does Sweden's new psychological defence agenda fit within the contemporary international counter-disinformation and counter-hybrid fields?

This report takes its point of departure in this crowded policy area to offer a contemporary interpretation of the concept of psychological defence. It builds upon the work of the Lund University Psychological Defence Research Institute and the research groups that preceded it, that have been actively developing operational and conceptual support for Sweden, the UK, EU institutions, NATO, and the Hybrid and Strategic Communication Centres of Excellence in Helsinki and Riga for almost a decade. This report represents our view of how the policy area stands and where it is heading. It is one interpretation of which there are likely to be many. This interpretation has been developed in dialogue with the Psychological Defence Agency; however, all positions are the responsibility of the authors and do not reflect any official stance.

To achieve this, the report observes two key threads. The first is a historical continuity perspective; that is to say, a perspective grounded in the origins and Cold War practices of psychological defence in the Swedish context. The second is from a contemporary policy perspective; an approach centred on the domestic and international debates and practices responding to the post-2014 security environment and finding conceptual clarification and purpose from that updated context.

The report begins with a brief summary of the history of the concept, followed by an exploration of how psychological defence fits within contemporary policy debates and terminologies. It then explores contemporary psychological defence through four overlapping principles: resilience, threat intelligence, deterrence, and strategic communication. It examines these principles as constitutive of contemporary psychological defence, including a brief assessment of the best practices currently in use internationally in each area. In brief, the principles are:

Resilience
Coordinated efforts to foster societal resilience and reduce vulnerabilities in people, systems, and institutions.

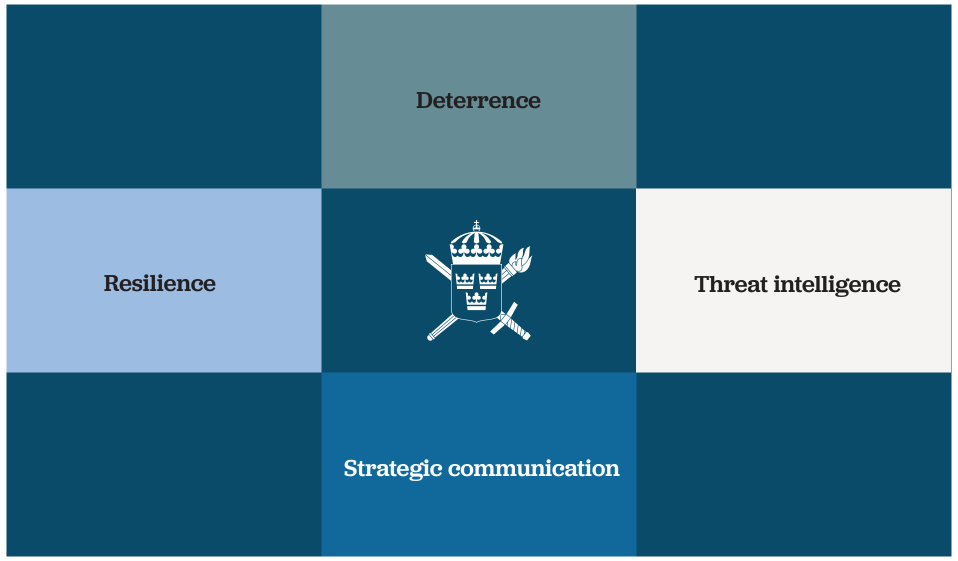
Threat intelligence
Coordinated efforts to understand and track external threats.

[1] Foreign Information Manipulation and Interference.

Deterrence
Coordinated efforts to defend society and, where possible, shape the behaviour of external threat actors.

Strategic communication
Coordinated efforts to understand and counteract vulnerabilities and threats through engagement in the information environment.

We situate the Psychological Defence Agency, the main public body with responsibility for psychological defence, at the centre of these four principles. When we speak of coordinated efforts, MPF has the mandate from government to act as the principal coordinator for many of these issues. It does not do all the tasks itself, but has responsibility for how they are defined, conducted, and organised. It is the hub within government collecting expertise and capabilities in how psychological defence contributes to these areas. Other agencies have specialised roles within different parts of these areas.



The first principle, **resilience**, focuses on the capabilities a country can draw upon to reduce its vulnerabilities and protect its population in times of peace, crisis or war. It is closely tied to questions of civil defence, protection of critical infrastructure, and crisis preparedness. From a psychological defence perspective, it covers the resilience of people and institutions, understanding of risk, and the ability to encourage personal responsibility through for example media literacy and the will to defend. It acknowledges gaps in the knowledge of one's own society, for example the grievances that make some social groups distrustful of others, such as social exclusion. It is heavily focused on domestic cooperation and a whole-of-society approach to resilience through collaboration between public, private, and civil society institutions.

The second principle, **threat intelligence**, focuses on better understanding the nature of the threat. It seeks to understand the influence techniques that threat actors deploy. From a psychological defence perspective, it is focused upon monitoring foreign propaganda and developing effective methods for analysing, investigating, and sharing insights about trends. On the one hand, it is heavily engaged with understanding threat vectors, such as the assets, technical opportunities, behaviours, and contexts that are used to undermine the information environment. On the other, it is focused on understanding specific threat actors, their intentions, capabilities, opportunities, and resources, and ensuring that these profiles are kept up to date.

The third principle, **deterrence**, focuses on the political and operational measures a country has available to protect its population and where possible mitigate the behaviour of threat actors. It is closely tied to questions of diplomacy, international alliances, and security policy. From a psychological defence perspective, it is focused upon the assessment of threats combined with political decision-making about the extent to which it is possible to change the calculus of a threat actor by, for example, raising the costs of their harmful activities by exposing them. It is heavily focused on international cooperation because alliances are often more effective at counteracting the efforts of a hostile actor than one country alone.

The fourth principle, **strategic communication**, focuses on the ability to prepare, respond, and shape the information environment to minimise the impact of hostile foreign propaganda on public deliberation. From a psychological defence perspective, it is focused on understanding the ecosystem in which communication related to foreign interference takes place, including research about media systems, algorithms, and patterns of information consumption, and using this knowledge to inform effective countermeasures. It is focused on understanding the audiences targeted by foreign propaganda, and where possible educating and informing them about known risks and threats. As such, it constitutes a continuous dialogue both with one's own society and with threat actors, emphasising resilience on the one hand, and deterrence on the other.

In summary, this report outlines a contemporary reimagining of psychological defence predicated on the opportunities that the new Psychological Defence Agency affords. It focuses on how the concept of psychological defence must adapt to shifting geopolitics and technological environments. It lays out four principles—resilience, threat intelligence, deterrence, and strategic communication—that serve as a comprehensive framework for the broad array of societal actors who fall under the psychological defence umbrella. As such, the report defines and develops upon the concept of psychological defence for the 2020s and beyond, in the context of debates about a potential new European-level institution performing a similar role.

2 | The concept of psychological defence

2. The concept of psychological defence

The political use of the concept of psychological defence in Sweden can be traced to two strands of thought. The first is the idea of psychological warfare. Propaganda was considered a key form of psychological warfare, albeit one that had advanced during and after the Second World War to the extent that it was increasingly drawing upon innovations associated with the public relations and advertising industries. These were seen as producing more direct effects upon the cognitive faculties of the public, boosted by the new media technologies of the time. The fear of what these new techniques could achieve was palpable in the reports at the time, although the assessment of effects may perhaps in hindsight seem overplayed (See e.g., SOU 1953:27).

A second strand of how the term came to be used in a Swedish political context is through association with Freudian psychoanalysis. The notion of psychological defence mechanisms originates with the work of Sigmund and Anna Freud, with the latter systematising and popularising the concept from her father's work in the 1930s (Freud 1936). Identifying ten techniques that people often unconsciously use to protect themselves from anxiety-inducing thoughts or impulses, some defence mechanisms are considered part of healthy behaviour, while others are associated with neuroses. Later research has identified dozens of mechanisms and categorised them according to their sophistication or level of pathology (Bailey & Pico 2022). Certainly, at the time psychological defence came to be used in Sweden as a political concept, Freudian discourse was widely discussed even if not directly referred to in official reports about psychological defence. The similarities, in terms of an unconscious response to threatening external influences, are striking, although many of these ideas entered the debate indirectly through the work of Swedish military psychologist Torsten Husén (Bennesved & Cronqvist 2023).

Origins

During the First World War, Sweden had no state information service. The notion that Sweden should have a central organisation in charge of war-related information dates to the 1920s but was never prioritised. During the Second World War, the State Information Board (Statens informationsstyrelse – SIS) was established. In addition to having a broad mandate for information control, it was expected to counter foreign propaganda and manage public opinion (Rossbach 2017; Tubin 2003). According to Rossbach (2017), SIS engaged in what can be regarded as domestic propaganda. The goal was to strengthen Sweden's values and democracy during the war, as a counterweight to the psychological warfare targeting the country from the Great Powers. However, early efforts to develop defensive wartime information operations were considered heavy handed.

A core task of SIS was to counter anti-Swedish propaganda. This was done in part by reviewing private telegrams, letters, and telephone calls, as well as monitoring the mass media. Infamous "grey notes" could then be distributed to media houses outlining recommendations on what was considered appropriate for publication (SOU 1953:27, p. 9). Public criticism made an interventionist and censorship-based approach to psychological defence politically untenable. Less controversial activities, such as working through local representatives, measuring public opinion, supporting grassroots organisations, developing educational correspondence courses, as well as pamphlets and booklets outlining what to do in the event of war, were considered more successful examples of how defensive wartime information operations could function (Rossbach 2017).

In 1948, a public inquiry was launched into how Sweden should organise its post-war counter-foreign propaganda activities. Former Minister of Internal Affairs Eije Mossberg presented a public inquiry in 1953 entitled Psychological Defence (Psykologiskt försvar – SOU 1953:27). The Inquiry went on to be known as the Mossberg Report, which is often credited with invention of the term Psychological Defence.[2] Mossberg stated,

> *"For a small country which seeks to avoid war and does not prepare attacks against anyone, it is natural to – if the war does come – use the psychological means of combat for psychological defence" (SOU 1953:27, p. 16).*

Psychological defence would henceforth become a formal component of Sweden's total defence doctrine.

The inquiry proposed that a Preparedness Commission for Psychological Defence should be established, with the task of readying the wartime organisation of psychological defence. To increase the public's awareness of foreign propaganda, a two-pronged strategy was proposed. On the one hand, the public would be immunised against propaganda and its main techniques. "A particular problem offers the question of immunisation against enemy propaganda and against other forms of psychological warfare. Undoubtedly, some results can be achieved by teaching people to recognize propaganda, to be critical of rumours, and to distinguish between false and genuine messages", the inquiry stated (SOU 1953:27, p. 63). A second area of focus was on increasing the public's willingness to resist invasion and strengthening the will to defend (SOU 1953:27; Cronqvist 2019). For this, a crucial point was that the quality of life for Swedes had to be sufficient that they would be willing to fight to defend it.

[2] Historian and Director General of MPF Dr Magnus Hjort has traced the first usage in relation to Swedish security policy to an article in Swedish Daily SVD 1941-01-29.

Consolidation

The subsequent consolidation of the psychological defence agenda saw it used essentially as an inverted version of psychological warfare; i.e., psychological defence is the action required to counteract an enemy's psychological warfare. The term was acceptable politically. "Defence" suited Sweden's neutrality. The combative term "war" was avoided. It didn't contain the words "press" or "media", which helped to set it apart from the heavily criticised SIS. The obscure nomenclature contributed to the effort's initial ability to maintain a low-but-not-secret profile (Rossbach 2017, pp. 54–55). It also made sense in terms of funding. Sweden lacked the resources required for sophisticated military psychological warfare. Psychological defence efforts were supposed to be small during peacetime and only grow in case of escalation or conflict.

The Mossberg Report served as the foundation for the new public agency, the National Preparedness Commission for Psychological Defence (Beredskapsnämnden för psykologiskt försvar – BN). BN received its first instruction in October 1954 (SFS 1954:628). The Authority's primary responsibility was to oversee contingency planning for psychological defence in case of war. This included preparing a large readiness organisation to allow the government and central authorities to communicate with media houses to counter an adversary's psychological warfare. BN had no peacetime information responsibilities. It was a civilian agency under the Ministry of Defence. It was led by a civilian, and its board of directors included politicians, journalists, public officials, and academics (SOU 2020:29). In addition to the main task of preparing and planning for operations in the event of war, BN studied Swedish public opinion, foreign propaganda directed at Sweden, and monitored Swedish information activities relevant to psychological defence preparedness. It was also responsible for collaborating with other relevant bodies for these pursuits (SOU 2020:29; Cronqvist 2019).

Alongside BN, the National Centre of Public Information (Statens upplysningscentral – UC) was formed. In wartime or during heightened tensions, UC was responsible for coordinating public information. UC was a much larger organisation of 630 people. There was also a network of civilian professionals who were prepared to support UC's work, including over 100 advertising creatives handpicked from leading bureaus, and regionally based civil servants prepared to serve as liaisons between county councils and the public (Swedish Armed Forces n.d.). The main purpose of UC's activities was "to preserve and strengthen the population's willingness to defend itself and its spirit of resistance, and to promote Swedish interests in foreign public opinion" (SOU 1953:27, p. 245). In cooperation with the media, UC's job was to ensure that the public was continuously provided with accurate information about the military, the supply chain, and matters of special importance. It would also "monitor the public mood in the country", "follow and analyse foreign propaganda", "counter psychological warfare directed against the Swedish people", "in cooperation with military bodies, plan and, during a state of war, take psychological measures directed against the enemy", and in other ways strengthen the population's spirit of resistance (SOU 2020:29, p. 48).

Distinguishing between tasks in war and peace was a dilemma for the psychological defence organisations. The natural role of the BN, it was argued, was war planning and research, not peacetime information tasks. Therefore, in 1962, an additional institution, the National Defence Committee on Public Information (Totalförsvarets Upplysningsnämnd – TUN), was established as a civilian sister authority with the task of supporting and coordinating public information on security policy and the increasingly complex Swedish total defence project (SOU 1961:18; SFS 1962:310).[3] Books, films, and brochures aimed at the public, not least schoolchildren, were its main forms of communication. One concrete task that the Board was responsible for from the outset was the advertisement of the preparedness brochure *If War Comes* (Om kriget kommer) in the country's telephone directories (SFS 1975: 892; SFS 1983:482).

During the 1960s and 1970s, as these practices became increasingly institutionalised, psychological defence referred to three primary tasks. The first was to detect and counteract the effects of propaganda and other foreign powers' attempts to unduly influence Swedish public opinion. The second task was to ensure that accurate and up-to-date information could be obtained by the authorities and the public, even in difficult circumstances such as crisis and war. This was in essence a form of crisis preparation involving media and military and civilian spokespersons. The third task was to monitor and help to strengthen the population's ability to resist external threats and willingness to defend Sweden (Petersson 2018). These three tasks formed the core of the concept of psychological defence during its 'golden age'.

Decline & re-establishment

BN, TUN, and UC were merged in 1985 to form a new centralised authority, the Psychological Defence Board (Styrelsen för psykologiskt försvar – SPF). SPF's main task was to lead and coordinate the planning of the country's psychological defence, to disseminate knowledge about security policy and total defence, and to promote and coordinate information from other authorities in these fields. In the event of a state of emergency or war, or otherwise by special decision of the Government, SPF also had the task of maintaining and strengthening the population's willingness to defend and its spirit of resistance, as well as managing contacts between media and key spokespersons (SFS 1985:476; Tubin 2003). However, this reorganisation meant that in the wartime organisation, the number of staff was reduced to just over 300 by the mid-1980s, whereas SPF had around 10 staff (Tubin 2003). As time passed, greater distance was encouraged toward journalists to encourage media independence.

Until the end of the Cold War, Sweden carried out extensive work in the field of civil defence. As a result of the improved security situation in the early 1990s, civil defence began to be phased out, as did large parts of the planning for the heightened state of crisis and war. Resources previously devoted to national defence were redirected to international peacekeeping and humanitarian operations, as well as to strengthening the capacity to prevent and respond to severe crises and stresses on society in peacetime (SOU 2021:25). A considerable amount of research commissioned by SPF focused upon crisis communication and the role of media during crises and war. In 2000, the expanded Information Office within the Government Offices absorbed the SPF's press centre, and SPF became predominantly a funder of research (Tubin 2003). In 2002, certain responsibilities were transformed to the newly established the Swedish Emergency Management Agency (KMB) (Krisberedskapsmyndigheten) (SFS 2002:518). When the Swedish Civil Contingencies Agency (Myndigheten för samhällsskydd och beredskap – MSB) was established in 2009, SPF and KBM were discontinued. MSB's directives gave them responsibility to support the coordination of information provided to the public and the media in the event of a crisis or war (SFS 2008:1002).

[3] This was a more complex process, which Hjort (2004) contends had roots in political conflict.

For the next decade, the concept of psychological defence was mostly only used in reference to the Cold War. However, a small unit was created in MSB in 2016 to deal with the growing informational threat that had been observed in Estonia, Georgia, and Ukraine among others, and that became global headline news in conjunction with November 2016's US Presidential Election. On 16 August 2018, the Swedish Government decided on the directives for a new committee with the purpose to make proposals for a new authority with overall responsibility for the development and coordination of psychological defence (Dir. 2018:80). The inquiry, *En ny myndighet för att stärka det psykologiska försvaret* (SOU 2020:29), which issued its report in May 2020, concluded that it was unclear whether the many public agencies tasked with psychological defence had sufficient knowledge of each other's work. As a result, it proposed the establishment of a new public agency with the mission of coordinating the work of identifying, analysing, and responding to undue information influence directed against Sweden or Swedish interests.

According to the inquiry's findings, the purpose of psychological defence should be to protect an open and democratic society, freedom of expression, and Sweden's freedom and independence (SOU 2020:29). In line with Sweden's security policy, upholding sovereignty and maintaining territorial integrity were predicates of the country's security objectives (Prop. 2014/15:109). The inquiry claimed that a strong total defence should include psychological defence as a crucial component carried out in both peacetime and war (SOU 2020:29).

Furthermore, the inquiry argued that Swedish independence and autonomy, democracy and the free expression of opinions and views, as well as trust and confidence in the institutions of society, must be protected by the psychological defence (SOU 2020:29). In the inquiry, various types of attacks and threats to the values that the psychological defence should aim to protect were described. Cyber-attacks and disinformation directed against Swedish authorities, politicians, companies, and other Swedish targets were particularly emphasised. Additionally, attempts to influence elections, covertly or overtly, and threats and rumours directed against politicians, officials, researchers, journalists, media companies, and others, were described as significant concerns (SOU 2020:29).

A key function of psychological defence was therefore defined as the capability to identify, analyse, counter, and prevent malign information influence activities and other misleading information aimed at Sweden or

Swedish interests. Therefore, a national psychological defence capability must be able to recognise, evaluate, combat, and prevent such activities on a national and international level. The resilience and willingness of citizens to defend themselves would also be a key part of this. Aside from the new agency, other authorities would take responsibility for much of this work. The report recommended that the new agency would be tasked with overseeing coordinated efforts and advancing capability development. The agency, according to the inquiry, should be positioned as Sweden's central collaboration and expertise hub for psychological defence (SOU 2020:29). On 1 January 2022, the Psychological Defence Agency (Myndigheten för Psykologiskt Försvar – MPF), was established.

Continuity & change

In the 70 years since the concept and practice of psychological defence was established, much seems to have changed. Annex 1 provides an overview of the main tasks conducted by each of the psychological defence bodies up to and including MPF. Put briefly, the post-war history of psychological defence in Sweden reveals that the following functions remain constant:

- The need for a national coordination body tasked with convening actors and expertise.
- The centrality of scientific research, including surveys and opinion polls, as foundational knowledge for psychological defence.
- A function committed to informing and educating the public about known external threats.
- The need for understanding and analysis of the propaganda that targets Sweden.
- Preparation for a more advanced psychological defence capability in case of crisis and war.

In the more recent formulation of psychological defence, some divergences also appear:

- In line with Sweden joining the European Union, and more recently NATO, international cooperation is now central to psychological defence-related activities.
- Due to the development of digital media and cybersecurity, advanced technical analysis of propaganda through open-source intelligence (OSINT) is now a point of focus.
- The mandate for countering foreign propaganda, either directly or as a support function for other actors, is more pronounced.
- The role of explaining Swedish security policy to the public has been reduced to making the public aware of operational concerns, such as specific influence campaigns.

These insights provide key points of departure for reimagining the concept of psychological defence for the 2020s. However, we must also consider more recent international policy developments in closely related fields since Sweden and the MPF do not exist in isolation. Most importantly, it is critical to understand the ways in which Sweden has engaged with international partners in the years during which the concept of psychological defence was out of favour, in order to better understand the role it can play in a rapidly evolving toolset of capabilities and policy options.

3 | Evolution of the field

3. Evolution of the field

Although psychological defence was no longer high up on the agenda from the mid-1990s onward, Sweden continued to perform an active and progressive role in the international community's work on countering disinformation. The deteriorating European security situation witnessed an escalation of confrontations with Russia, most seriously the 2014 annexation of Crimea and the Russian-led hybrid war conducted by 'little green men' (unmarked militia) in the Donbass. The Kremlin intensified its propaganda war against the West, leveraging an amplified presence in the European media environment to earn political support while seeking to undermine the coherence of EU foreign policy (European Parliament 2016). Interference in the 2016 US Presidential Election (European Parliament 2018; European Parliament 2023), 2017 French Presidential Election (Conley & Jeangène Vilmer 2018; Daniels 2017), and the 2017 Catalonian referendum (Rankin 2017) among others raised the sense of urgency to counteract these types of threats. At its meeting in 2016, the World Economic Forum identified online warfare and disinformation as one of the top ten global risks (World Economic Forum 2016), raising it to the single greatest short-term global risk in 2024 (World Economic Forum 2024).

Policy developments

Following the EU's 2015 directive to address Russian disinformation, many member states acknowledged the dissemination of false narratives and deceptive information concerning EU politics, facilitated predominantly through social media platforms. This directive prompted the establishment of the East Stratcom Task Force within the European External Action Service (EEAS), a specialised unit that departed from the norms of EU diplomacy by directly naming and shaming the spreaders of pro-Kremlin disinformation (European Union External Action 2021a). The 2018 Code of Practice on Disinformation and Action Plan Against Disinformation, and the 2020 European Democracy Action Plan established new policy instruments as counter-disinformation activities ramped up around Europe (European Commission 2018; European Parliament 2020; Pamment 2020a). Likewise, in the US, the 2017 National Defense Authorization Act provided the basis for the Global Engagement Center (GEC) to act as a central hub for coordinating United States government efforts to counter disinformation (Hall 2017). 2017 also saw the launch of the NATO-EU European Centre of Excellence for Countering Hybrid Threats, while the NATO Strategic Communications Centre of Excellence had been active since 2014.

In 2016, the Swedish Civil Contingencies Agency (MSB) was mandated to establish a capability to identify and respond to undue information influence and other dissemination of misleading information. These policy areas were defined as

> *"Information influence, or cognitive influence activities, by foreign actors carried out with the aim of influencing the perceptions, behaviour and decision-making of target groups to the advantage of foreign powers."*
> **(MSB 2017 in SOU 2020:29).**

Many of MSB's counter-information influence activities were about increasing awareness of the problem and creating an understanding of what information influence is (MSB 2018). One illustrative example of their work was the publication *If Crisis or War Comes* (2018) sent to every household in Sweden, an allusion to the Cold War pamphlet *If War Comes*. A second example was *Countering Information Influence Activities – Handbook for Communicators* (MSB 2018), which developed into a national training programme initially in support of protecting the 2018 General Election.[4]

In mustering its capabilities to protect the 2018 General Election, Sweden was seen as an innovator within the field (LaForge 2020; Fjällhed, Pamment & Bay 2021). Sweden was an active participant in international policy debates, alliances, and capability development in this area; for example, seconding a national expert to the NATO Strategic Communications Center in Riga since September 2016, as well as secondees at EEAS and the Hybrid COE working on disinformation and foreign interference related issues. Sweden participated in many international networks related to these issues, and provided training to partner states, particularly those in Eastern and Central Europe. The MSB team dealing with undue information influence would become the core staff of the new Psychological Defence Agency.

[4] The training programme is still ongoing. See Sörenson & Pamment (2023) for a recent summary and evaluation of the training.

Terminology

One of the points of concern during this period was a lack of conceptual clarity over the nature of the challenges faced by governments in this area. While popular culture characterised the new media landscape as corrupted by "fake news", the emerging international policy area was initially characterised by the term "disinformation". However, over time it has become clear that use of the term disinformation as a catch-all is both problematic and misleading. The establishment of psychological defence as an alternative conceptualisation for the policy area in the Swedish context is therefore a significant development of the policy area, with potential consequences for international partners. It is these consequences that the following section explores in greater detail.

In our conceptualisation, use of the term disinformation has been shorthand for three overlapping groups of problems. 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. The second group of problems is the more complex phenomena of influence campaigns driven by motivated organisations capable of coordination, using multiple communication tools, and conducting clandestine activities. Such coordinated activities are often referred to as operations or campaigns to emphasise the complex and opaque nature of the planned influence effort. 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 our view, these groups of problems overlap, but are distinct to the degree that different actors should be involved in monitoring, educating, and responding to the threats.

The first group of problems (mis-, dis-, and mal-information, or MDM) can be characterised by an emphasis on specific pieces of information content spread by individuals who are exercising their freedom of speech but are factually incorrect. NATO (2020) defines disinformation as the 'deliberate creation and dissemination of false and/or manipulated information with the intent to deceive and/or mislead'. Although often mistakenly used to cover the entire policy area related to information-based interference, disinformation is best understood as part of a group of closely related terms focusing on two factors: the factualness (or truthfulness) of a message, and the likely intent behind the creation of the message. Misinformation refers to verifiably false information that is shared without an intent to mislead, whereas malinformation refers to true or partially true information that is twisted or taken out of context to support false interpretations (Pamment 2021; Pamment, 2022a). Together, the three terms cover many of the problematic issues associated with a digital public sphere, in which false information circulates without the checks and balances that traditional media provide.

Disinformation & associated concepts

Term	Misinformation	Disinformation	Malinformation
Definition	Threat intelligence	False information created intentionally	False information distorted intentionally
Operational components	Truth/factualness of content Intent of content creator		
Counter-measure capabilities	Content correction capabilities Public resilience-building capabilities		
	• Content correction • Fact-checking • Debunking • NGO Networks "Elves"	• Public resilience • Media literacy • Public awareness campaign • Prebunking	

For many countries including 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. In the US Department of Homeland Security, for example, mis/dis/mal is referred to collectively as MDM (See e.g., Department of Homeland Security 2022). Disinformation is the more widely recognised term, albeit often as a loosely prescribed synonym for the legal term 'information influence' (Sweden) or its international equivalents (see below), or as a more general reference to false or misleading content with a meaning gliding between mis/dis/mal. Disinformation has, for example, been used in this manner in official government documents such as the regulatory letters outlining the mandates of MPF and the Swedish Institute, as well as other government statements (See e.g., Dir 2018:80; SFS 2015:152). In more recent international debates, MDM increasingly represents an approach to factchecking and debunking from a health of democratic debate perspective, which in practice means an emphasis on increasing public participation and reducing political polarisation. Countermeasures are often seen as the remit of civil society, such as journalists, nongovernmental organizations, tech platforms, think tanks, and academia in order to avoid the perception that government acts as the arbiter of truth. Tasks such as factchecking, debunking, content moderation, media literacy education, and source criticism are seen as key methods for improving the overall health of the public sphere from MDM (Pamment & Lindvall Kimber 2021).

The second group of terms focuses on more complex campaigns in which a hostile actor coordinates a variety of illegitimate communication techniques to influence target groups to their benefit. Encouraging the spread of mis-, dis- and mal-information may be among the methods used. The Swedish term information influence (*informationspåverkan*) is used to encapsulate efforts to influence democratic processes using illegitimate, but not necessarily illegal, methods to the benefit of a hostile external power. It emphasises the communication techniques that make up a coordinated effort to influence a society, their manipulative components, and the objectives of those conducting them (Pamment et al., 2018). Similarly, terms such as information manipulation (used by France and EU institutions) and influence operations (preferred for example by tech companies) define coordinated efforts to influence that often make use of clandestine techniques, and that ultimately seek to benefit the source and/or cause harm to others (Jeangéne Vilmer et al., 2019).

Term	Information Influence	Information Manipulation	Information Operations
Definition	Illegitimate communication intended to influence society to the benefit of hostile foregin powers	Coordinated efforts involving the diffusion of false or distorted information with the intent to cause political harm	Coordinated efforts to manipulate or corrupt public debate for a strategic goal
Operational components	Intent to cause harm to the benefit of hostile actor Use of multiple illegitimate communication techniques Negative interference in public debate Covert coordination		
Counter-measure capabilities	Analysis and identification capabilities Strategic communication capabilities		
	• Analysis & identification • Monitoring • Investigation • OSINT	• Strategic communication • Counter-narrative • Counter-brand • Published analysis	

Information influence & associated concepts

This group of terms has stronger policy and institutional support insofar as they have a clearer legal basis. France has adopted information manipulation into law (Guillaume 2019), and the EU recently integrated the most important principles into its Foreign Information Manipulation & Interference (FIMI) policy (Council of the European Union 2022).[5] Tech companies refer to influence operations and coordinated inauthentic behaviour in their policies for content removal and attribution (See e.g., Facebook 2021). The

[5] "The EEAS defines FIMI as a pattern of behaviour that threatens or has the potential to negatively impact values, procedures and political processes. Such activity is manipulative in character, conducted in an intentional and coordinated manner. Actors of such activity can be state or non-state actors, including their proxies inside and outside of their own territory." https://www.eeas.europa.eu/eeas/tackling-disinformation-foreign-information-manipulation-interference_en

Swedish term "undue [or unwarranted] information influence" covers influence efforts with a connection to foreign powers (state or nonstate) and provides the legal basis for government institutions to take countermeasures toward such campaigns where there is a clear external dimension (Andersson, 2023). The fundamental principle of this group of activities is the idea of a concerted, often clandestinely organised campaign with objectives that benefit the source and/or seek to cause harm to others. It is no longer a question of factchecking or debunking individual messages, but rather of understanding how messages fit within broader narratives and developing the means to counter those narratives. Approaches to dealing with this category of problem emphasise the capability to analyse, uncover, and counteract the behaviour of established threat actors.

The third group of concepts focuses explicitly on foreign interference. This area builds upon the themes covered in the concepts of MDM and influence campaigns by adding two additional factors. First is the assumption that the activities within this category, no matter who conducts them, are carried out on behalf of a hostile foreign power, ultimately with some form of state backing. Second, the communication activities broadly considered to be under foreign interference go beyond information per se and overlap with the broader categories of hybrid, cyber, or other state threats including espionage (Ördén & Pamment 2021). This imparts an additional layer of complexity upon information influence that positions the communication activities within a set of (often) covert tools for generating geopolitical influence.

Term	Foreign interference
Definition	Disinformation, information influence, and other hybrid influence methods conducted by or on behalf of a hostile state actor
Operational components	Intent to cause harm to the benefit of hostile actor Use of multiple illegitimate communication techniques Negative interference in public debate Covert coordination; Deployment in coordination with other hybrid influence methods
Counter-measure capabilities	Intelligence: collecting processing, and use capabilities Security Policy: actor-specific capabilities
	• Intelligence • All-source • Intelligence sharing • Counterintelligence • Security policy • Deterrence • Attribution • Legislation

Foreign interference

Foreign interference has the strongest legal and institutional support insofar as it is tied to military and civilian intelligence, counterintelligence, protection of critical infrastructure, and bilateral relations with hostile states. NATO and the EU have developed significant tools to deal with sub-threshold activities, most prominently cyber and hybrid, with the EU cyber sanctions regime and NATO announcements that cyberattacks and hybrid interference can trigger Article 5 (NATO 2024). The EU sanctions against Russian state media during the Ukraine invasion indicate the intensification of legal countermeasures to foreign interference through information influence (Council of the European Union 2022; Pamment 2022b). The EEAS' FIMI policy attempts to combine the three groups referred to in this section in a manner which helps to broaden the policy area from "disinformation" to influence campaigns and hybrid foreign interference (European Union External Action Service 2021b). However, it does so in a broad manner that does not necessarily capture the nuanced distinctions between problem groups.

While the distinctions are not always neat (for example, it is often unclear who is behind MDM activities or how they fit into broader campaigns), we argue that distinguishing these three problem sets is necessary to explaining how and why psychological defence can become a key concept for this field in the coming years. Most importantly, the concept and implementation of psychological defence in the Swedish example demonstrate important opportunities for the international debate, which we outline in the following sections.

Gaps and opportunities

International terminology has in recent years developed from referring to the policy area simply as "disinformation", to developing more nuanced terms such as FIMI, capable of better defining the nature of the problem that policies seek to remedy. As discussed above, for the sake of clarity these problems can be broadly grouped into MDM, which focuses on the truthfulness and intent of content from a public participation perspective; influence campaigns, which emphasises coordination and illegitimacy by capable organisations; and foreign interference, which emphasises state actors behind influence campaigns and the broader bilateral relationship with them. The recent EU concept of FIMI is well-placed to capture this general policy development as it covers all three groups, albeit without the nuance to distinguish appropriate capability development and ownership for the different components of the problem. However, it is less obvious where psychological defence fits into this apparatus.

The first clear contribution that psychological defence makes to the disinformation policy area is with the fundamentally defensive role of the concept. Psychological defence is what states do to protect their populations from psychological warfare. It is a contribution to civilian defence anchored upon protection of fundamental freedoms such as freedom of thought and freedom of expression from external interference. As such, it is profoundly aligned with promotion and protection of the values and principles of liberal democracy. MPF currently describes these fundamentals as:

- A free, critical, and independent media
- A well-informed and well-educated population
- A society based on trust and cohesion, between people and the government.

One benefit of dividing the disinformation policy area into three sets of problems is to make a clear distinction between protection of the domestic sphere and the fundamental freedoms of a population, from the actions of manipulative organisations and hostile states. This means in practice that the Psychological Defence Agency does not have a mandate to intervene in the mis-, dis- and mal-information group of problems, only to provide capacity-building support and advice to civil society, the media, and other government agencies affected by this type of problem. This group of problems is, at its core, fundamentally connected to building societal resilience.

For many countries, including most prominently the US, a lack of clarity about boundaries within the disinformation policy area has allowed some defensive actors to become entangled with domestic political polarisation. In January 2023, the Republican-controlled House Judiciary Committee subpoenaed information about the counter-disinformation activities of a variety of prominent US universities, think tanks and companies, on the grounds that these activities may be politically motivated (Myers & Frenkel 2023). A similar political controversy was faced by EUVSDISINFO in 2018, when three Dutch media outlets took the EEAS to court for labelling their articles as pro-Kremlin disinformation. The resulting political debates eventually reached the settlement that EUVSDISINFO would not include domestic European outlets in its database of pro-Kremlin disinformation (See e.g., Pamment & Ahonen 2023). It is therefore of fundamental importance to emphasise that psychological defence has the mandate to strengthen the capabilities of civil society and not intervene in domestic political debate. In other words, the critiques levelled against some US researchers and EUVSDISINFO cannot be applied to Swedish psychological defences actors. The conceptual focus on external actors performs an important role in insulating the policy area from the threat, risk, and accusation, of unintentional domestic political interference. The concept of psychological defence has a clear advantage due to its historical basis as a defensive function against external threats, and hence provides a politically bipartisan direction to the policy area.

The second contribution to the policy area is that psychological defence offers an unambiguous strategic umbrella to a variety of capability-building issues connected to the disinformation policy area. A major problem in many countries is the division of labour between government institutions, as well as across civil society and the private sector, regarding mandates and responsibilities (Pamment 2020b; Andersson 2023; Pamment & Ahonen 2023). Some government agencies can only get involved if there is a suspicion of criminal activity. Others, if there is a risk of threat to critical infrastructure, to military targets, to national security, or to diplomatic relationships. Others are focused on promoting freedom of speech and the integrity of public debate. In the Swedish case, creating a Psychological Defence Agency to coordinate and enhance whole-of-society capabilities makes some small steps toward a more coherent response to the policy area that still respects these differences.

Likewise, the concept provides an umbrella for establishing coherent countermeasures across the problem-sets defined in these terms, as well as between mandated actors. Some countermeasures are best levied by journalists or researchers (e.g. fact checking and debunking), others by diplomats, intelligence agencies, or militaries (e.g. attribution and deterrence). Traditions differ by country. Some actors like to be visible, others less so. Some actors determine countermeasures according to business priorities, others by geopolitics, others by ethical imperatives or their organisations' raison d'être. In this context, it is difficult if not impossible to define a single toolbox of countermeasures or anticipate their consistent application. Psychological defence provides an umbrella for countermeasure capability development that can potentially rationalise and strengthen the national response. When positioned as a (civil) defence reflex, psychological defence can help to set the boundaries of the countermeasure toolbox, as well as the objectives and strategies used to manage external threats.

Furthermore, psychological defence provides an umbrella for rationalising and advancing capabilities within the disinformation policy area. This includes monitoring and investigation standards, training and capacity-building, management of national and international alliances, and concept and doctrine development. A particular focal point is around open-source intelligence techniques (OSINT) with regard to data collection and analysis, as well as strategic communication for building societal resilience, deterring threat actors, and developing countermeasures. This is particularly valuable as the activities of threat actors evolve; capability development is an ongoing concern. For example, the strong overlap between hybrid, cyber, and espionage with influence operations suggests that the FIMI policy area may increasingly encompass a holistic approach to foreign interference. Psychological defence is relevant across these stovepipes, augmenting capabilities as a force multiplier.

The value of a concept such as psychological defence is precisely that it offers a strategic direction to a diverse collection of actors loosely working in the national interest to combat the three groups of problems encompassed by this policy area. It takes those three problem areas and offers a conceptual basis for how the policy area can be managed in such a way as to maximise defensive capabilities while also protecting fundamental freedoms. In light of these gaps and opportunities, the decision was made to create the Psychological Defence Agency in 2021. Its job has become to grasp these opportunities and to implement them.

The Psychological Defence Agency

The Psychological Defence Agency opened its doors in January 2022. In accordance with its mandate (SFS 2021:936), MPF is responsible for leading the coordination and development of the actions taken by authorities and other actors in Sweden's psychological defence, providing support for such actions, and helping to increase the population's resilience during times of peace as well as heightened states of alert. In addition to helping to increase the population's resilience, the agency also aids regional authorities, local authorities, businesses, and nongovernmental organisations. The agency's mandate includes identifying, analysing, preventing, and countering foreign malign information influence activities and other disinformation directed at Sweden or at Swedish interests. MPF is also tasked with improving the population's capacity to recognise and counteract deceptive propaganda campaigns. Thus, psychological defence should contribute to societal resilience and a desire to defend the nation.

MPF initially reported to the Ministry of Justice, but as of January 2023 is based under the Ministry of Defence. It consists of three departments. The Operations Department (Operativa avdelningen – OA) locates, investigates, and combats foreign disinformation campaigns that are hostile to Sweden or Swedish interests. This entails creating reports and analyses about specific circumstances, threat actors, and societal vulnerabilities as well as suggesting appropriate countermeasures. The Capability Development Department (Förmågehöjande avdelningen – FH) works to improve and expand society's overall capacity for psychological defence. This entails primarily development of research, training, and international partnerships to support the Swedish populace, government organisations, municipalities, media, non-profit defence groups, the private sector, and civil society while also facilitating improved coordination between these actors. An administrative department provides support for MPF in areas such as human resources, budgeting, strategic planning, legal issues, facilities, security, and communication.

The mandate of MPF is to lead the work of coordinating and developing the activities of the public authorities and other actors in Sweden's psychological defence in peacetime and at high alert (SFS 2021:936 §1). In particular, MPF is tasked with promoting cooperation between authorities and other actors in prevention work and to create conditions for and contribute to coordinated operational action (SFS 2021:936 §2). The coordinating role does not imply that MPF should take over decision-making powers on matters which should be decided by other authorities (SOU 2020:29).

This is based on the principle of devolved responsibility, which the Government explains as,

> *All actors involved should be responsible for identifying and addressing information influence within their respective areas of responsibility"*
> **(Prop. 2016/2017:1, Expenditure Area 6, p. 60).**

Instead, coordination means ensuring that essential aspects of the work do not fall through the cracks, that there is no unnecessary duplication of effort, that the authorities affected by an incident are aware of each other's information and interpretation of the situation, and that there can be a coordinated response from Swedish authorities if necessary (SOU 2020:29).

As such, within Sweden's psychological defence, all authorities are responsible for countering information influence in their area of operation and cooperating with other relevant authorities for an effective response. This is currently managed through an informal cooperation structure with the other public agencies sharing responsibility for psychological defence, which is led by MPF (MPF/2023:56). Agencies meet in Director General, Operational, and Long-term capability building working groups (See Annex 2).

Areas for psychological defence cooperation & participating organisations (2024)	
Military defence & security	• Ministry of Defence • Swedish Security Service (SÄPO)
Civil defence & resilience	• Civil Contingencies Agency (MSB) • County Administrative Boards
Media & information literacy	• Swedish Agency for the Media
Global communication & the image of Sweden	• Swedish Institute

Included in the mandate of MPF is the responsibility to report to the Government any information on undue information influence and other dissemination of false or misleading information that may be relevant to national security or that for any other reason should be brought to the Government's attention (SFS 2021:936 §4). For this, MPF conducts media monitoring and interacts with other authorities. This can include the analysis of online information sources financed and/or directed by foreign actors that target information influence activities against Sweden or Swedish interests (ISS 2020). MPF may receive relevant intelligence briefings under Section 2 of the Defence Intelligence Act but is unable to direct intelligence collection, pending the results of an inquiry due to report in 2024 (SFS 2022:120).

Since launching in January 2022, unexpectedly high levels of information influence against Sweden have thrust MPF into the limelight. Beginning late 2021, an information influence campaign targeting the Swedish social services and The Care of Young Persons (Special Provisions) Act (LVU), garnered international attention. The campaign falsely claimed that the Swedish social services were involved in the abduction of children, particularly targeting Muslim families. Initially, much of the communication was spread by people in Sweden through Arabic language social media channels as well as physical demonstrations. Social media content began to accuse the Swedish Government of being a fascist state that placed Muslim children in Christian homes with paedophiles and forced them to consume alcohol and change their names and religious beliefs (Ranstorp & Ahlerup 2023). The campaign spread rapidly in Arabic-language news and social media, leading to widespread mistrust among Muslims both in and outside of Sweden, and evolving into what has been termed the most extensive influence campaign ever to target Sweden (Ranstorp & Ahlerup 2023; Government Office of Sweden 2023).

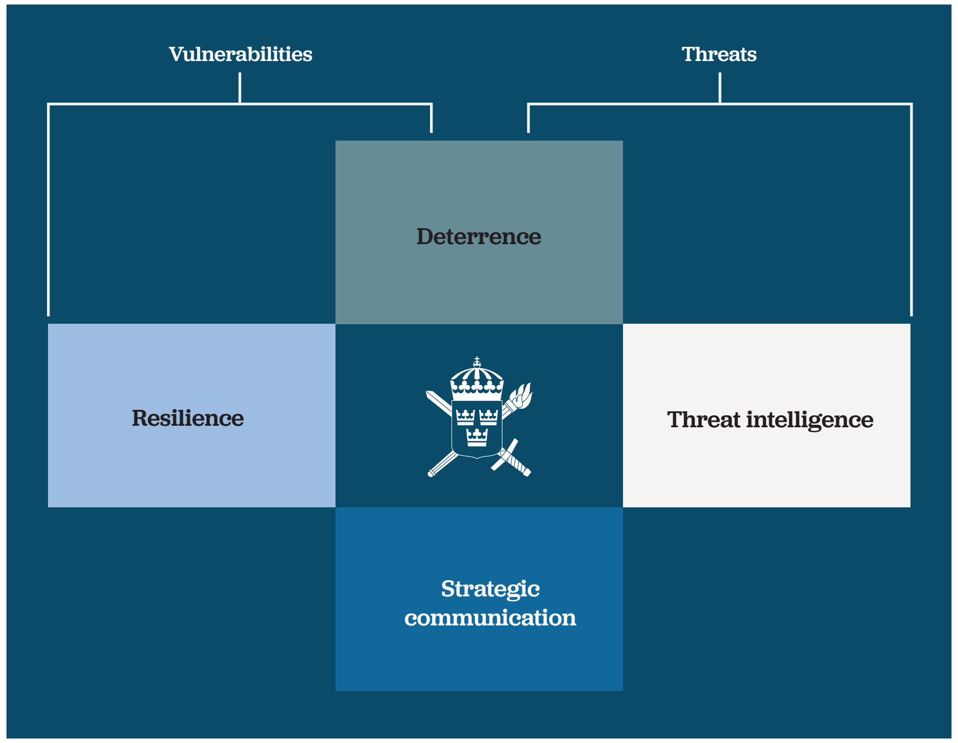
This and other campaigns against Sweden have sought to depict Sweden as anti-Islamic, attempted to derail Sweden's NATO membership (Prime Minister's Office 2022), and contributed to elevating the risk of terrorism both domestically and for Swedish citizens abroad (Ministry of Defence 2023; The Swedish Security Police 2023). In response to "the greatest foreign, security and defence policy challenges of modern times", the Swedish Government announced its intention to establish a National Security Council at the Prime Minister's Office and appointed Henrik Landerholm, Director General of MPF at the time, as the country's first National Security Adviser in November 2022 (Prime Minister's Office 2022). The Government also handed MPF the additional task to combat malign information influence targeting Sweden in connection to burnings of the Quran by individuals associated with far-right groups in July 2023 (Ministry of Defence 2023). In August 2023, Sweden elevated its terror alert to the second-highest level in response to the Quran burnings and threats from militant groups. It marks the first time since 2016 that Sweden has raised its terror alert to such a level (Ministry of Justice 2023).

4 | Principles of the new psychological defence

4. Principles of the new psychological defence

During the Cold War, psychological defence had a reasonably stable meaning intimately bound to Sweden's modest place in the post-War, and later bipolar, geopolitical order. When that geopolitical order broke down in the 1990s, the value of total defence, and with it psychological defence, diminished in favour of alternative capabilities such as crisis management. What does the present geopolitical context, and the overlapping concepts that have thrived in recent years, mean for the new psychological defence? In what ways do the new threat actors and manipulation techniques, new societal vulnerabilities and grievances, new security policy instruments and alliances, and new communication ecosystems prompt a reformulation of psychological defence's core principles?

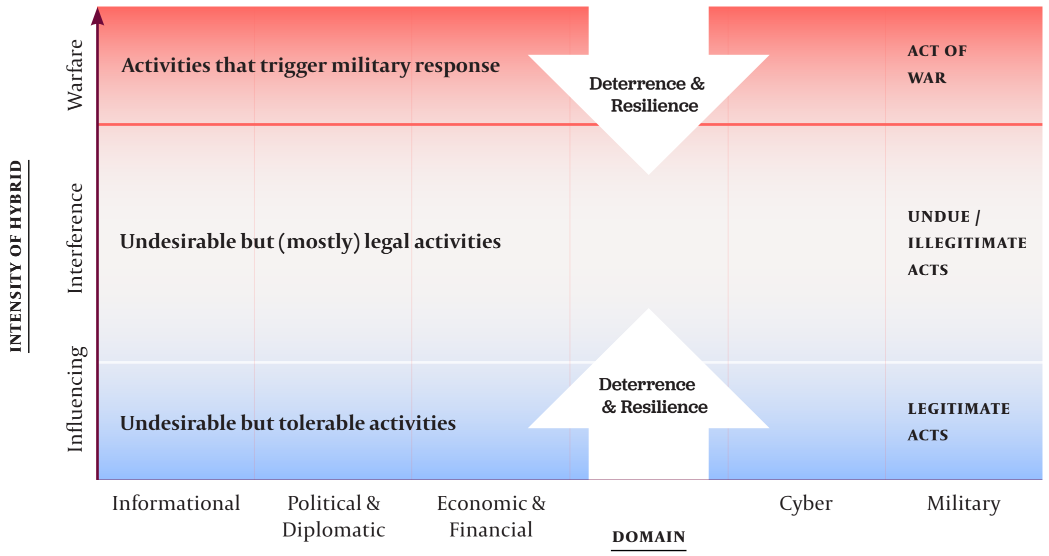
We argue that the contemporary understanding of psychological defence must acknowledge two poles: vulnerabilities and threats. Vulnerabilities are the weaknesses that exist in our society, our institutions, and in ourselves. Threats are the negative events, acts, or actors that exploit those weaknesses to achieve a goal. Current interpretations of Swedish legislation have operationalised these terms to mean *domestic vulnerabilities* and *external threats*. In other words, problems that are domestic in origin are vulnerabilities for national security since they belong to "us". Problems from abroad are categorised as threats. Psychological defence is mandated to try to reduce vulnerabilities and has some powers to tackle threats. Later sections will raise some of the issues with this operational division.



We argue that the new psychological defence is best conceptualised as comprising of four principles. The first two are *Resilience* and *Threat intelligence*, which correspond to the work on reducing vulnerabilities and analysing threats. In the middle, where the understanding of vulnerabilities and threats meet, are two further principles, *Deterrence and Strategic Communication*. Deterrence refers broadly to security policy work that seeks to develop policy positions for shaping the behaviour of adversaries in line with our understanding of the damage that their threat activities can have on society. Strategic communication is the understanding of the communication ecosystem as it relates to both threats and vulnerabilities and involves the development of strategies and tactics to implement security policy measures. The following sections expand upon these principles in detail.[6]

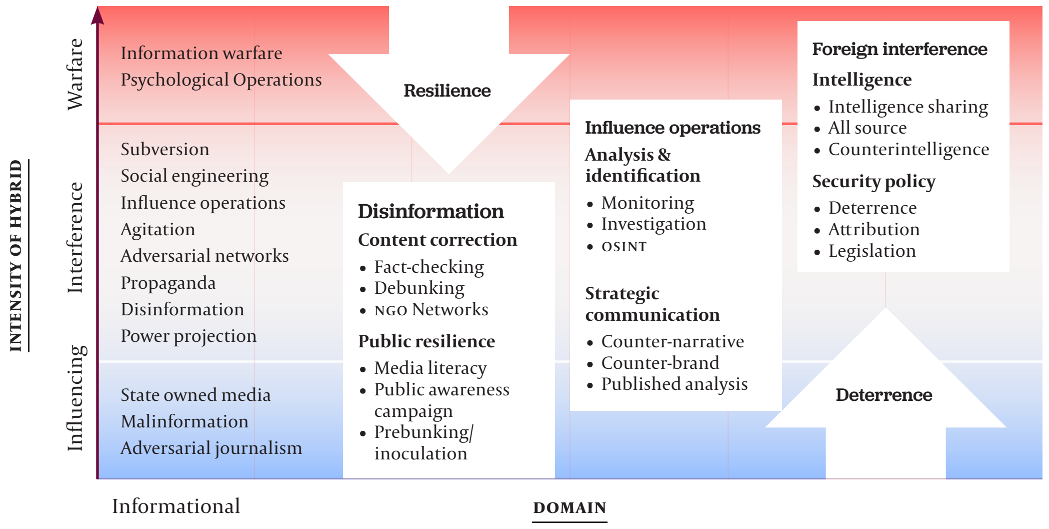
[6] MPF has a similar working concept where they place "Förmåga att agera" (Ability to Act) and "Vilja att försvara" (Will to Defend) in the middle of the four principles: Avhålla (Refrain), Varna (Warn), Agera (Act), and Stärka (Strengthen). They view these principles as effects and assert that defence capability should encompass threshold capacity (Refrain), early warning (Warn), societal resilience (Strengthen), and coordinated actions (Act). These effects constitute a comprehensive psychological defence capability.

Viewing psychological defence in this way requires a significant revision when compared to traditional conceptualisations. One way to visualise the approach is to plot out the threat landscape. Imagine the threat activities covered in the previous chapter (MDM, influence operations, and foreign interference) on a Y-axis that represents increasing intensity. At the lowest level are run-of-the-mill influencing activities that are generally seen as legitimate and hence acceptable to society, such as conducting public diplomacy or running an international news platform. Next is a grey area of threat activities that might constitute undue or illegitimate interference, up to a red line above which are hostile activities that would constitute an act of war. On the X-axis are domains such as *Information, Cyber,* and *Military,* which represent ways of grouping different threat activities by the sector in which they take place.



In such a model, resilience and deterrence can be positioned as a mindset designed to make unwanted threat activities harder to carry out. For example, increased resilience in the form of public education about source criticism can make it harder for mostly legitimate acts of influencing through an international state broadcaster such as Russia Today (RT) to find gullible audiences. Deterrence, for example in the form of timely attributions of threat actors carrying out subversion activities, can enact reputational damage that may dissuade a threat actor from continued agitation. Taken together, resilience and deterrence represent tools of statecraft to manage the threat landscape. However, to become effective, they must be utilised in a coherent and coordinated manner.

Psychological defence provides a significant part of that potential for the information domain, with some important spill over into other domains (Pamment & Palmertz 2023).



Such a visualisation allows for the major policy challenges outlined in the previous chapter to be positioned within the psychological defence umbrella. Problems connected to the first group of issues, mis-, dis- and mal-information, are at the lowest level of the chart, and are best met by capabilities such as fact checking and media literacy. MPF has a role in supporting NGOs, media, academics, and other government agencies in developing strategies for enhancing societal resilience through these methods. In the middle are problematic grey-zone threats such as influence operations, which are best countered using OSINT capabilities and counter-narratives. MPF has operational and long-term capacity-building capabilities designed to support Swedish society in this area. At the highest level are threats associated with foreign interference which require intelligence and security policy capabilities to counteract. MPF feeds into this work, though it is primary intelligence agencies, key ministries such as the Foreign Ministry and Ministry of Justice, and the Government Offices (including the new National Security Council) who take the lead on many of these activities.

By approaching the policy area in this way, the key components of psychological defence – resilience, threat intelligence, deterrence, and strategic communication – are organised as a whole-of-society effort to raise the cost of threat actions by strengthening and empowering society to resist.

Resilience

Hybrid threats target vulnerabilities in society, such as insufficient defences, under-resourced or under-developed capabilities, societal fissures and grievances, as well as gaps between institutional responsibilities (NATO 2024; Giannopoulos et al., 2021). The emergent term for capturing work on vulnerabilities within psychological defence is resilience. Resilience focuses on one's own proactive and defensive capabilities for minimising risk to a society. At its core, resilience has traditionally been about the capacity to endure and manage change, regardless of the circumstances. This is often referred to as the ability to 'bounce back' from sudden shocks, to adapt to changing realities, and to quickly restore some form of normality in the face of significant disruption (e.g., Swedish Defence Commission 2017, p. 1). It is closely associated with protection of the critical infrastructure that keeps a society functioning.

More recently, resilience has come to be repositioned as part of a holistic understanding of a society's resolve in the face of hybrid threats as well as traditional military threats and unexpected crises. It refers to the *routines, processes, and practices that empower the whole-of-society to participate in collective security* (Pamment & Palmertz 2023). It is centred on shared responsibility for security between a country's population, its public institutions, civil society, and private sector, and hence is a core facet of the long-term Swedish doctrine of *total defence*.

Resilience from a psychological defence perspective is agnostic about the source or nature of the threat; its focus is on the self. A society with better preparedness, fewer vulnerabilities, and effective crisis management is a less attractive target to hostile actors. Resilience is therefore not just a defensive concept since its resources simultaneously act as deterrents and raise the overall costs of efforts to disrupt a society. Recurrent themes therefore include a strengthening of:

Will to defend and spirit of resistance.

The concepts of "will to defend" (*försvarsvilja*) and "spirit of resistance" (*försvarsanda*) encompass more than just the individual readiness to protect oneself. Rather, the concepts are often viewed as being deeply entwined with the perception of the society one lives in, usually boiling down to fundamental questions such as: Is my way of life worth defending? It is often linked to citizens' trust in the state, authorities, and democratic institutions, which can differ based on various factors such as personal experiences, economic conditions, cultural background, and political beliefs. The hint of a spiritual dimension points to these factors as building upon nationalism and faith as well as logic.

Civil defence.

Civil defence "encompasses the whole of society and comprises the collective resilience in the event of war or danger of war" (Government Office of Sweden 2024).

Crisis preparedness.

This encompasses a wide range of activities, including emergency preparedness, disaster response, crisis management, and recovery efforts, aimed at safeguarding lives, property, and essential services.

Efforts to protect society's critical functions are determined through a prioritisation based on risk and vulnerability assessments. It is common for a country to monitor high priority societal vulnerabilities and to develop thresholds to inform about evolving threats. For example, adversaries might test computer sensitive networks at regular intervals, looking for avenues to infiltrate classified systems. Most countries quietly monitor these efforts and establish thresholds that would be triggered in case of a sudden intensification of hostile activity. The ability to create country-wide, and even internationally recognised, capabilities in these areas contributes to coherence, interoperability between different actors, and a common view of problems and solutions. Key capabilities include:

- *Risk assessment, vulnerability assessment* and *crisis contingency planning* for critical infrastructure and other crucial public services.
- *Monitoring* and *early warning capabilities* based around civil contingencies and crisis response.
- *Recognised security certifications* for organisations dealing with sensitive systems and other crucial processes.
- *Training and exercises* in crisis management coordination and response.
- *Whole-of-society participation* in shared capability development.

Following the experiences of total war during the Second World War, the Swedish doctrine of total defence focused on the ability of the whole of society to achieve common security goals. As a means of defending against psychological warfare and propaganda, psychological defence was positioned as the area of total defence that focused on protecting public debate and the information environment (SOU 1953:27). Associated capabilities included ensuring public awareness of global affairs, contingency planning for media systems in case of invasion, and preserving the public's will to defend the country.

Resilience is closely entwined with legal frameworks governing political participation. For example, Section 2 of the Swedish Constitution (RF), the European Convention on Human Rights (EKMR), the Freedom of the Press Act (TF), and the Public Access to Information and Secrecy Act (YGL), guide government agencies and other public entities in their responses to information influence under the principle of freedom of expression (Andersson 2023, p. 51–52). The objective is to protect democratic participation, and hence any countermeasures directed toward domestic target groups should value individual freedom of expression, promote balanced and objective communication, and align with legal frameworks and principles of psychological defence (Andersson 2023).

A fundamental focus of psychological defence since its origins has been on protection of free public debate. Since the Mossberg Report, it has been assumed that "results can be achieved by teaching people to recognise propaganda, to be critical of rumours, and to distinguish between false and genuine messages." (SOU 1953:27, p. 63). Resilience is, in other words, centred on developing people and institutions so that they can embody and enact a society's resolve. This remains a key principle of contemporary psychological defence. Contemporary approaches to improving resilience from a psychological defence perspective include:

- *Public awareness-raising campaigns*, such as public information campaigns about foreign propaganda and propaganda methods.
- *Efforts to improve media literacy*, for example by providing education or training in how to critically interpret media and especially content shared on social media.
- *Efforts to improve source criticism*, by encouraging people to critically evaluate information sources.
- *Support of credible journalism*, to foster a critical and independent media system based on established journalistic ethical norms.
- *Support of fact-checking initiatives*, by providing independent, nonpartisan reviews of mediated content for factual errors.
- *Support of debunking initiatives*, involving the targeted review of mediated content on specific topics or from certain sources to expose particularly politically motivated falsehoods.
- *Intelligence disclosures for the purpose of inoculation*, for example the "prebunking" conducted by the US and UK prior to the 2022 Russian invasion of Ukraine, which prepared the public for anticipated disinformation about the premise of the war.

Hence, the Swedish strategy for maintaining a robust psychological defence revolves around promoting a free media, bolstering citizens' resilience, and strengthening trust in state authorities (The Swedish Agency for Public Management 2017:5; MSB 2018). Much of this work is about strengthening democratic participation through media and information literacy. Raising awareness of the risk of cyberattacks and information influence campaigns is part of that work. For example, the campaign *Tänk Säkert*[7], endorsed by the MSB, the Police, and Stöldskyddsföreningen (SSF), strives to educate individuals on information and cyber security (MSB 2022b). The ongoing "Don't Be Fooled!" ("*Bli Inte Lurad!*")[8] initiative seeks to promote awareness and empower individuals to tackle deceptive and inaccurate information (Annex 3).

[7] https://sakerhetskollen.se/
[8] https://www.bliintelurad.se/

Threat intelligence

In recent years, the cybersecurity sector has established a form of intelligence work based around analysis of digital signals, behavioural markers, and contextual factors for the purpose of tracking threats. Often referred to as *threat intelligence*, this approach has provided much of the inspiration and language that has informed the burgeoning field of influence operations analysis. This includes some key concepts, institutional structures, data collection and analysis methods, as well as community standards. While cybersecurity is not the only field to have inspired contemporary approaches to influence operations analysis, there are many implicit adoptions, including:

- *A focus on identifying and tracking threat actors*. In cybersecurity, these are referred to as Advanced Persistent Threats, or APT. In analysis of influence operations, efforts are made to attribute campaigns to threat actors based on their known capabilities and interests.
- *Use of activity classifiers*. Cybersecurity analysis draws upon a series of standardised classifiers designed to facilitate data sharing within the defender community. Known as Tactics, Techniques and Procedures, or TTP, the classifiers enable coding of manipulation techniques in a manner that can for example reveal the connections between activities that comprise a cyberattack. In influence operations analysis, classifiers such as DISARM are currently in the testing phase and are high on the international agenda (See e.g., Newman 2022; The European Union Agency for Cybersecurity 2022).
- *Situational awareness informs strategic interventions.* Both fields rely on a strategic approach to monitoring threats, which may involve allowing threat actors to establish an infrastructure to better understand their goals and methods, compromise the threat actors, and/or remove all hostile assets at the same time. Usually, defensive and offensive counteroperations are clearly distinguished, and may even be conducted by entirely different teams.

It is worth underscoring that although cyberattacks and influence operations are often integrated from an attacker's perspective (for example, many cyber intrusions begin with an influence effort to persuade a target to click on an unsafe link), cyber and information influence attacks also have major differences. Most notably, while cyber techniques tend to fall into yes/no categories, influence is often ambiguous and intangible, and its effects often exist only in the perceptions of individuals. Efforts to directly adapt lessons learned from cybersecurity to influence operations are only ever partially applicable, and concepts from social scientific academic research, investigative journalism, and intelligence analysis, for example, remain essential to the field.

Perhaps the single most important overlap between fields is the importance of open sources to threat intelligence collection. Open-source intelligence, or OSINT, can at times seem marginalised in traditional intelligence studies literature (see e.g., Clark 2017). However, in cybersecurity, the "chatter" and other observable indicators across open sources on the internet provide important contextual insights into threat actor behaviour. Similarly, much online disinformation (or MDM), which can provide indicators of covert influence operations, plays out in the public sphere. At the same time, the Bellingcat effect[9], derived from mixing open-source methods with investigative journalism as well as creative methods of accessing restricted datasets, has in recent years significantly raised the profile of OSINT for a range of applications. Many of the leading think tanks, universities, companies, and NGOs working on the analysis of influence operations employ some form of OSINT methods, though the processes vary. The two main approaches may be characterised as follows:

Investigative research

Utilising methods from academic research, investigative journalism, and big data analysis, this approach combines advanced use of search engines, tech platform APIs, commercial digital monitoring platforms, and/or other specialist OSINT tools to identify and examine disinformation and influence operations. This can be supplemented by advanced tools and methodologies for e.g. digital forensics and network analysis.

Intelligence work using open sources

This approach follows the same rigorous processes used in secret intelligence analysis, and the results are often classified despite being derived primarily or exclusively from open sources. The main difference is not in the methods used, but in the fact that the work is planned, conducted, and distributed using the intelligence cycle. Secret intelligence, including cybersecurity data derived from signal intelligence, can be used to supplement or help to direct open-source collection and analysis. Such approaches are more likely to be used to identify and examine influence operations and foreign interference as a complement to secret intelligence, in order to more readily enable exploitation of the intelligence.

According to its current mandate, MPF is unable to direct collection of signals intelligence. It is not an intelligence agency, though it does receive regular briefings based on secret intelligence that can inform its data collection, analysis, and overall assessments (SFS 2022:120). Its work on situational awareness and threat assessment can therefore be described as threat intelligence based on OSINT and supplemented by secret intelligence. It follows the rigorous processes used by agencies working with classified intelligence. Swedish intelligence agencies sometimes conduct tasks that overlap with MPF's mandate of identifying and countering information influence activities from foreign powers, though their focus is on narrower instances connected to different mandates. MPF is the hub in the Swedish system for dealing with information influence from foreign powers, though it is a coordination position heavily contingent on interagency cooperation. Threat intelligence from the perspective of psychological defence may

[9] www.bellingcat.com

therefore be described as monitoring foreign propaganda and developing effective methods for analysing, investigating, and sharing insights about trends. On the one hand, it is heavily focused on understanding threat vectors, such as the technical opportunities, behaviours, and contexts that are used to undermine the information environment. On the other, it is focused on understanding specific threat actors, their intentions, capabilities, opportunities, and resources, and ensuring that these profiles are kept up to date. Overall, this implies the sharing of situational awareness between relevant societal stakeholders, including the Government Offices, public agencies, local government, the private sector, civil society, media and journalism, and the public. Exactly what is shared is different depending on the audience.

Threat intelligence can inform a variety of countermeasures (See e.g., Pamment 2022a) **including:**

Counterintelligence

A specialism in identifying domestic proxies who conduct information influence on behalf of hostile foreign states. For example, the FBI[10] includes disinformation alongside other aspects of foreign interference as part of its counterintelligence work.

Intelligence disclosures

Making conclusions or assessments from secret intelligence public in order to inform about and/or attribute threat activities.

Network disruption

Use of cyber capabilities to disrupt an adversary's network. For example, during the 2018 midterm elections, the US allegedly disrupted the internet access of the notorious St. Petersburg troll farm behind the 2016 election interference, the Internet Research Agency (Nakashima 2019).

Offensive operations

Run covert, coordinated influence operations abroad against a hostile state or its agents. MPF has the mandate to conduct offensive influence operations in the event of war.

[10] https://www.fbi.gov/investigate/counterintelligence/foreign-influence

Deterrence

Deterrence refers to coordinated activities that aim to shape adversaries' perceptions of cost and benefits to dissuade threatening behaviour (Keršanskas 2020). According to Schelling (1966, p. 2), the development of the nuclear deterrent during the Cold War contributed to a geopolitical environment in which "the art of coercion, of intimidation, and deterrence" became a core facet of military thinking. In the early-21st century, deterrence theory – traditionally seen as state-centric with Mutually Assured Destruction at its core – was applied to nonstate actors such as terrorist groups (David & Jenkins 2002), paving the way for its more recent application in areas such as cybersecurity and hybrid (see e.g. Pamment & Agardh-Twetman 2019). In its modern application, deterrence is usually divided into two areas: denial and costs. *Deterrence by denial* involves the reduction or removal of an adversary's capabilities and/or their intended effects. The three main denial areas are:

- *Denial of benefit,* reducing or removing the rewards anticipated from adversarial behaviour.
- *Denial of capabilities,* restricting or nullifying the threatening capabilities that the adversary can bring to bear.
- *Denial by punishment,* levelling punitive measures upon the adversary.

These *denial* options contribute to an overall approach to *deterrence by imposition of costs.* Deterrence by imposition of costs is a mindset and form of strategizing based upon the assumption that the collective impact of denial measures on the adversary's cost/benefit analysis will lead them to conclude that their aggressive actions are not worth it. In essence, it asks the question, *can we make this type of attack more costly to carry out?* Those costs might for example be in terms of a need for increased resources to carry out the harm (e.g., more people, advanced tools, and work hours are required), unanticipated costs to reputations (e.g. an increased risk of attribution and exposure (Pamment & Smith 2022), or highly damaging countermeasures (e.g. likelihood of offensive responses). While it is not always the case that the adversary acts rationally, at its core, deterrence by imposition of costs tries to make the harmful activity more costly (both metaphorically and actually) than the rewards that the adversary anticipates from its disruptive behaviour.

It is therefore essential to have some understanding of the adversary's decision-making processes, the resources they consider proportionate, and their own red lines or limitations. In other words, security policy experts need some understanding of the underlying historical and cultural context and frame by which the adversary views the world and interprets the strategies and actions of themselves and others. Some adversaries are more sensitive to certain types of costs than others; for example, it is often assumed that oligarchs are sensitive to economic sanctions and travel bans because of the expectation that wealth enables a luxurious international lifestyle. Others are acutely sensitive to attribution since they like to maintain a strongly positive reputation in public perceptions. Terrorists might be entirely unmoved by punitive or financial measures but respond to theological reasoning. Understanding what makes the adversary tick requires intelligence about their psychological make-up, motivations, information sources, and decision-making processes (Pamment & Palmertz 2023; Pamment & Agardh-Twetman 2019; Pamment 2020c).

The ability to attribute is a fundamental component of the deterrence capability. According to a recent report published jointly by the Hybrid COE and NATO Stratcom COE, attribution consists of three types of evidence: technical, behavioural, and contextual, supported by a legal and ethical assessment (Pamment & Smith 2022). *Technical evidence* focuses on the trail of signals generated by illicit activities, such as IP addresses or telemetry. *Behavioural evidence* focuses on the manipulative activities and techniques, including Tactics, Techniques & Procedures (TTP). *Contextual evidence* examines the content and political elements of the interference campaign, such as messaging and narratives. Finally, the *legal and ethical* assessment weighs up crucial questions of proportion, data protection, and geopolitical strategy related to using these different kinds of evidence.

Each type of evidence can be subdivided by the types of data sources used. In each evidence category, data can be collected through *open sources* (e.g. through research and OSINT), *proprietary sources* in which the data has commercial ownership (e.g. social media platform backends and private sector intelligence), and through *classified secret intelligence* (e.g. SIGINT and HUMINT). In February 2023, Microsoft's threat intelligence team published a white paper in which they adopted the framework for explaining future public attributions (Microsoft's digital Threat Analysis Center 2023). To develop effective deterrence including countermeasures, it is necessary to assess the evidence as to who is behind the activities, what resources they have access to, what their overall opportunities for influence are, and what their intentions may be. This can help to create an overall threat assessment drawing on threat intelligence, an appreciation for the bilateral relationships between key actors, and an assessment of risk based on known vulnerabilities.

Deterrence in the context of influence operations draws upon a toolbox of countermeasures designed to shape the behaviour of a threat actor. It is intimately connected to resilience, in the sense that known vulnerabilities provide a level of insight into what behaviours can be accepted and which must be averted; to threat intelligence, in the sense that all knowledge of adversary intentions, resources, opportunities, and behaviours feed into an assessment of risk and priority; and to strategic communication, in the sense that many deterrence actions are directly or indirectly communicated to an adversary, whether through e.g. signalling, attribution, intelligence disclosures, or awareness raising. Deterrence is, in other words, the security policy function that draws together and provides strategic direction to the psychological defence apparatus. Countermeasures can include:

- *Signalling:* communicating to a hostile actor awareness of their behaviour or sending a message that their behaviour will not be tolerated, through indirect means. For example, an intelligence agency stating that a foreign actor is seeking to undermine the national interest, without naming that actor, signals awareness without escalation.

- *Deterring:* coordinated efforts to influence a hostile state's calculus. For example, during the Sweden's NATO accession period, the UK signed a mutual protection pact and sent the HMS Queen Elizabeth to the Baltic to demonstrate resolve.
- *Attribution:* technical and political capabilities to assign blame to states and their proxies. For example, following the Salisbury Poisoning, Prime Minister Theresa May stated in Parliament that it was "highly likely" that Russia was behind the poisoning.
- *Legislation:* specific laws that empower government agencies to act proactively. For instance, Australia has the National Security Legislation Amendment (Espionage and Foreign Interference) Act 2018 and Singapore has the Foreign Interference (Countermeasures) Act.
- *Sanctions:* levy costs upon hostile state and its agents. Example: in March 2022, the EU imposed sanctions on Russian state media, including RT and Sputnik, in response to disinformation spread about Ukraine prior to and during the invasion (Council of European Union 2022).

Strategic communication

To operationalise resilience, deterrence, and threat intelligence into cohesive countermeasures, strategic communication plays a key role. This role is so fundamental that communication should be considered a principle of psychological defence in its own right, in addition to being a tool of implementation. Building societal resilience relies upon a continuous and inclusive dialogue between Government, civil society, the private sector, and individuals. Threat intelligence involves continuous scanning of the information environment, categorisation of threats, and information exchange between countries, government agencies, civil society, and the private sector across intelligence stovepipes. Deterrence implies a continuous dialogue between antagonists and one's own government, as well as within and between allied governments for coordination purposes. This is more than simply communication, and rather encompasses a commitment to being communicative.

> *Strategic communication encompasses all communication that is substantial for the survival and sustained success of an entity. Specifically, strategic communication is the purposeful use of communication by an organization or other entity to engage in conversations of strategic significance to its goals*
> **(Zerfass et al., 2018, p. 493).**

The idea of strategic communication as a tool of management is useful, since it emphasises that it is a means to an end; in this case, a means to operationalising the policy of psychological defence. It is not possible to implement resilience, deterrence, and threat intelligence without planned and credible communication. In other words, strategic communication is both a tool to influence internal populations, external threats, and to improve coordination within and between government agencies and other key stakeholders. The strategic communication process is designed to use data to inform decisions to achieve a desired effect. Most strategic communication models therefore emphasise at a minimum the following steps[11]:

- *Goals:* Based on policy aims, define what the communications activity intends to achieve with a focus on desired outcomes. This may include behavioural change.
- *Insight:* Using social scientific research tools including big data, surveys, market research, grassroots communication, and intelligence, identify the targets of the communication intervention and their characteristics, information sources, belief patterns, and grievances.
- *Strategizing:* Use the insight to develop a strategic plan based upon a theory of change (what you believe will happen as a consequence of your activities), and including appropriate messaging, channels, and partners.
- *Implementation:* Conduct the communication activities according to the strategic plan. In most cases, implementation involves a strong dialogical component.
- *Assessment:* Weigh up whether the strategic communication activities achieved the desired results, often in dialogue with stakeholders. This is often seen as part of a cycle, feeding back into the communication process.

From this perspective, many countermeasures are essentially strategic communication interventions designed to shape behavioural change of some kind. For example, countermeasures associated with mis-, dis- and mal-information often take the form of information campaigns. This may include factchecking low-level disinformation and developing public education initiatives, with the goal of changing how groups and individuals consume information, or building trust and developing or repairing reputations. Countermeasures associated with influence operations emphasise social listening, audience insights, and developing powerful counternarratives for the purpose of shedding light on clandestine influence campaigns. Countermeasures associated with foreign interference emphasise information sharing to support a purposeful dialogue with threat actors, with the aim of changing the calculus of adversaries. Planned and coordinated communication is the key to an effective response.

For example, guidance from MSB (2018) and the UK Government Communication Service (Pamment 2021) outline a series of proactive and reactive communication tools such as:

- *Inoculation:* communication interventions designed to proactively debunk ("pre-bunk") false messaging before it has become widely spread.
- *Awareness raising:* efforts to proactively shape public debate about issues likely to be subjected to mis- and disinformation.

[11] See e.g., the OASIS Framework, https://gcs.civilservice.gov.uk/wp-content/uploads/2020/03/Guide-to-Campaign-Planning-OASIS-Framework.pdf

- *Information campaigns:* a planned sequence of communications and interactions that uses compelling narratives over time to deliver a defined and measurable outcome, such as behaviour change.
- *Network building:* shaping networks of likeminded allies and organisations to provide a safe space for solving problems together.
- *Counter-branding:* a range of communicative activities that collectively seek to ensure a reputational cost to actors who persistently spread false, misleading and harmful information.
- *Resilience building:* the aim of resilience building and media literacy initiatives is to empower people to better understand how false information can be spread on and offline, so that they can more effectively engage with what they see, read, and hear.
- *Debunking:* when false or manipulated information is circulating and you wish to counteract the impact of the false information by asserting the truth.
- *Counter-narratives:* countering narratives involves exposing falsehoods and contradictions in how important issues are explained to different audiences and where possible replacing them with a more truthful narrative.
- *Crisis communication:* managing reputations and ensuring that accurate information reaches target audiences as it becomes available.

As noted throughout this report, countermeasures can also include a broad array of activities that involve policy innovations, physical interventions, symbolic actions, deterrence acts such as signalling, good governance programmes, and better coordination. The strategic communication component emphasises that all such activities should be planned from a communicative perspective. This is challenging in most countries due to the difficulties of cross-governmental coordination, as well as the multiple layers of cooperation required with civil society and the private sector in civil defence. In Sweden, cross-governmental coordination has an additional level of complication due to the unique public agency system, which does not allow for ministerial rule and hence makes coordination more challenging. MPF currently runs the governmental cooperation structure which is based upon voluntary participation (Annex 2). In addition, the Government Offices – as well as individual ministers – often communicate on psychological defence issues in coordination with MPF. For example, in January 2023, Sweden's Prime Minister, and the head of the Psychological Defence Agency (MPF) Operations Department disclosed an ongoing foreign influence campaign aimed at manipulating public opinion and decision-making processes regarding Sweden's potential NATO membership (Prime Minister's Office 2023).

An important question is whether it is desirable for MPF to act as both an intelligence agency and an agency that communicates regularly and openly with domestic audiences. There is a strong argument to suggest that it cannot do both. An agency that relies predominantly on OSINT is more able to communicate its findings quickly and with greater nuance. However, for that to be effective, its communication must still be closely aligned with the Swedish intelligence agencies. This is challenging because their communications have different goals. Traditionally, intelligence agencies communicate infrequently and benefit from some of the highest levels of public trust among government agencies (See e.g., Medieakademin 2023; Slick et al., 2023). An agency like MPF, however, exists to take greater risks in its communication; to communicate more often, with greater agility, and at times based upon lower levels of certainty. It could then be seen as a cross-governmental communications hub for the Swedish intelligence and security policy agencies and departments on questions of information influence, assuming coordination would work effectively.

Other areas of activity relevant to strategic communication include developing and maintaining an up-to-date understanding of how traditional media, social media platforms, evolving technologies such as Artificial Intelligence (AI) and Machine Learning (ML) (Fredheim & Pamment 2024), and non-traditional platforms such as video games (See e.g., Pamment, Falkheimer & Isaksson 2023) function and behave. This may involve regular contact with industry. The aim is to understand the information environment infrastructures used both by individuals and by threat actors, and potentially how they can also be used to disseminate trustworthy information. It also involves understanding media systems, their governing policies, and the consumption habits of their users. This is fundamental to understanding audiences.

5 | Prospects for the new psychological defence

5. Prospects for the new psychological defence

This report demonstrates that psychological defence is well-placed to contribute to international debates in the field of disinformation and hybrid policy. By fitting these issues into the broader context of civil defence, the mandates and functions can be considerably sharpened in comparison to the relatively ambiguous notion of disinformation. By distinguishing between problem sets (MDM, Influence Operations and Foreign Interference) and designing a whole-of-government approach centred on raising costs, psychological defence sets a compelling vision that can shape the international agenda in this area. In particular, we emphasise the centrality of protecting fundamental freedoms such as freedom of thought and expression to the concept. While this is usually one of the main concerns of those working with the disinformation policy area, psychological defence goes further in codifying these principles and compelling all activities to fit within the spirit of these fundamental freedoms. The distinction between threats and vulnerabilities is key to this.

All domestic issues related to psychological defence are formulated as vulnerabilities, which means that capacity-building is often the main solution. If portions of your own population believe in things that are untrue, or get their information from untrustworthy sources, that is a societal vulnerability. They should not be treated as threats; rather it is the responsibility of the government and society as a whole to improve access to services that can empower the population. The approach has some similarities to public health initiatives. Countermeasures for vulnerabilities also go beyond strategic communication to include symbolic actions and physical actions. This means that many existing programmes and tools associated with good governance, particularly those seeking to improve the lives of the domestic population as well as programmes that improve life for foreign citizens, often form the heart of the solution. Psychological defence involves rethinking a very broad set of governance tools within the mindset of resilience and deterrence.

Work which targets the domestic population is focused on strengthening democracy by:

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

Work which targets external threat actors is focused on deterring threat activities by:

- Developing the capability to map, track and attribute threat actors
- Understanding evolving threat behaviour
- Maintaining alliances
- Raising the cost of threat activities
- Developing countermeasures to directly push back on threat activities.

The distinction between domestic vulnerabilities and external threats is not entirely without problems. For example, many societal actors fulfil a double function in which they may be simultaneously "domestic" (i.e., based in Sweden or a national of Sweden) and "external" (i.e. behaving as part of the formal or informal networks of threat actors). While it is necessary in such circumstances to treat these actors as vulnerabilities given that their domestic rights supersede other concerns (unless, for example, they are considered a criminal, counterintelligence, or counterterrorism threat), the lack of mandate for MPF and Swedish intelligence agencies to study the domestic information environment in depth is a potential blind spot. While this insulates the domestic public sphere from government encroachment upon freedom of speech, in practice there is the significant risk that domestic debate becomes degraded because it is vulnerable to exploitation by threat actors targeting this gap. Adversaries often have a better analysis of societal vulnerabilities than a government is permitted to produce. In other words, while the psychological defence approach solves many fundamental problems of the disinformation policy area, there remain areas of ambiguity that the concept – as it is formulated here – is not able not resolve.

On the threat side, traditional stovepipes within the intelligence community also provide substantial hurdles to creating effective psychological defence capabilities. Threats are adaptive, and often responsively seek out gaps and ambiguities between institutions and established capabilities (Nilsson, Weissmann & Palmertz 2024). MPF's role in the Swedish intelligence community is not yet clear. Furthermore, the responsiveness of the IC to cross-cutting issues such as hybrid threats is slow, with multiagency taskforces difficult to create. As conceptualisations of threats develop, psychological defence is, in our view, increasingly likely to be positioned at the intersection between information, cyber, hybrid, and espionage. The present informal cooperation structure for psychological defence is an important starting point for addressing some difficult questions in the coming years, such as:

- *Early warning.* The ability to leverage situational awareness to support early warning is key to broadening the possible range of countermeasures. However, distinguishing between signals and noise is challenging, particularly if an agency is not mandated to monitor domestic discourse in any detail. The result is that many developing vulnerabilities will only be discovered once they have evolved into large enough threats to be noticed.
- *Stovepipes.* National intelligence systems are effective at creating stovepipes between analytical areas to protect secrets. However, many contemporary threats, such as hybrid, cyber, espionage, and influence operations are designed precisely to seek out the gaps between institutional coverage and skillsets. Creating MPF as a hub for information influence does not immediately resolve interagency coordination issues, particularly in cases where information influence is intimately connected to more prioritised foreign interference issues.
- *Mandates.* Connected to stovepipes is the difference in mandates between intelligence agencies. For example, in Sweden MPF cannot monitor domestic public debate, whereas intelligence agencies have that mandate if there is suspicion of a crime, or if there is a threat to national security. While the mandates at times seem to overlap, in other instances there are gaps in coverage and knowledge.

Despite these challenges, it is worth underscoring that psychological defence in its current formulation is a new task, in a new geopolitical context, with many new opportunities to grow and evolve. While its history provides some lessons and continuity, and recent international policy developments offer direction and momentum, many of the crucial details are not yet resolved. Input from EU and NATO allies, as well as from debates in Brussels about an EU-level psychological defence function, are likely to add many new ideas and possibilities to the discussion.

References

References

Andersson, A. (2023). *Rättsligt ramverk för bemötande av informationspåverkan – En studie av det rättsliga ramverket för bemötande av informationspåverkan genom informationsåtgärder.* FOI-R--5443--SE. Retrieved from https://www.foi.se/rapportsammanfattning?reportNo=FOI-R–5443–SE

Bailey, R., & Pico, J. (2022). Defense Mechanisms. In *StatPearls [Internet]*. Treasure Island (FL): StatPearls Publishing. Retrieved from https://www.ncbi.nlm.nih.gov/books/NBK559106/

Bennesved, P., & Cronqvist, M. (2023). En humanistiskt skolad kunskapsstrateg på ett samhällsvetenskapligt fält: Torsten Husén och framväxten av ett svenskt psykologiskt försvar. In J. Östling, A. Jansson, & R. S. Stringberg (Eds.), *Humaniora i välfärdssamhället: Kunskapshistorier om efterkrigstiden* (pp. 241–265). Kriterium.

Braw, E. (2022, December 8). Create a Psychological Defence Agency to Prebunk Fake News. *Prospect Magazine*. Retrieved from https://www.prospectmagazine.co.uk/politics/create-a-psychological-defence-agency-to-prebunk-fake-news

Conley, H., & Jeangène Vilmer, J. (2018, June 21). Successfully Countering Russian Electoral Interference. *CSIS Briefs*. Retrieved from https://www.csis.org/analysis/successfully-countering-russian-electoral-interference

Council of the European Union. (2022.) *Council conclusions on a Framework for a coordinated EU response to hybrid campaigns*. Retrieved from https://www.consilium.europa.eu/en/press/press-releases/2022/06/21/council-conclusions-on-a-framework-for-a-coordinated-eu-response-to-hybrid-campaigns/

Council of the European Union. (2022). *EU imposes sanctions on state-owned outlets RT/Russia Today and Sputnik's broadcasting in the EU*. Retrieved from https://www.consilium.europa.eu/en/press/press-releases/2022/03/02/eu-imposes-sanctions-on-state-owned-outlets-rt-russia-today-and-sputnik-s-broadcasting-in-the-eu/

Cronqvist, M. (2019). Mediekunskaper och propagandaanalyser : Beredskapsnämnden för psykologiskt försvar och PROPAN-projektet 1970–1974, in Norén, F., & Stjernholm, E. (Red.) (2019). *Efterkrigstidens samhällskontakter.* (Mediehistoriskt arkiv; Vol. 43). Mediehistoria, Lunds universitet.

Daniels, L. (2017, April 23). How Russia hacked the French election. *Politico.* Retrieved from https://www.politico.eu/article/france-election-2017-russia-hacked-cyberattacks/

Davis, P., & Jenkins, B. (2002). *Deterrence and Influence in Counterterrorism: A Component in the War on al Qaeda,* RAND Corporation, Retrieved from http://www.rand.org/pubs/monograph_reports/MR1619.html.

Department of Homeland Security. (2022). *DHS Needs a Unified Strategy to Counter Disinformation Campaigns.* Retrieved from https://www.oig.dhs.gov/sites/default/files/assets/2022-08/OIG-22-58-Aug22.pdf

Dir. 2018:80. *En ny myndighet för psykologiskt försvar.* Retrieved from https://www.regeringen.se/contentassets/b4b90c231b4144e683d5b4a594fe27b1/en-ny-myndighet-for-psykologiskt-forsvar-dir.-201880

European Union External Action Service. (2021a). *Tackling disinformation: Information on the work of the EEAS Strategic Communication division and its task forces (SG.STRAT.2).* Retrieved from https://www.eeas.europa.eu/countering-disinformation/tackling-disinformation-information-work-eeas-strategic-communication-division-and-its-task-forces_und_en?s=2803

European Union External Action Service. (2021b). *Tackling Disinformation, Foreign Information Manipulation & Interference.* Retrieved from https://www.eeas.europa.eu/eeas/tackling-disinformation-foreign-information-manipulation-interference_en

European Commission. (2018). *EU Code of Practice on Disinformation.* Retrieved from https://digital-strategy.ec.europa.eu/en/library/2018-code-practice-disinformation

European Parliament. (2016). *Report on EU strategic communication to counteract propaganda against it by third parties.* Retrieved from https://www.europarl.europa.eu/doceo/document/A-8-2016-0290_EN.html

European Parliament. (2020). *European Democracy Action Plan.* Retrieved from https://www.europarl.europa.eu/legislative-train/theme-a-new-push-for-european-democracy/file-european-democracy-action-plan

European Parliament. (2018). Kremlin trolls in the US presidential election. *At a Glance.* Retrieved from https://www.europarl.europa.eu/thinktank/en/document/EPRS_ATA(2018)614700

European Parliemant. (2023). Foreign interference in *EU* democratic processes: Second report. *At a Glance.* Retrieved from https://www.europarl.europa.eu/RegData/etudes/ATAG/2023/747908/EPRS_ATA(2023)747908_EN.pdf

Facebook. (2021). *Threat Report The State of Influence Operations 2017-2020.* Retrieved from https://about.fb.com/wp-content/uploads/2021/05/IO-Threat-Report-May-20-2021.pdf

Fjällhed, A., Pamment, J., Bay, S. (2021) A Swedish Perspective on Foreign Election Interference. In Hollis, D & Ohlin, J.D. (eds) *Combatting Election Interference: When Foreign Powers Target Democracies.* Oxford University Press

Fredheim, R. & Pamment, J. (2024) Assessing the risks and opportunities posed by AI-enhanced influence operations on social media. *Journal of Place Branding & Public Diplomacy*

Freud, A. (1936). *The Ego and the Mechanisms of Defence,* London: Hogarth Press and Institute of Psycho-Analysis

Giannopoulos, G., Smith, H., & Theocharidou, M. (2021). *The landscape of Hybrid Threats: A conceptual model.* The European Centre of Excellence for Countering Hybrid Threats. Retrieved from https://www.hybridcoe.fi/publications/the-landscape-of-hybrid-threats-a-conceptual-model/

Government Offices of Sweden. (2023). *Government taking strong action against disinformation and rumour-spreading campaign.* Retrieved from https://www.government.se/press-releases/2023/02/government-taking-strong-action-against-disinformation-and-rumour-spreading-campaign/

Government Offices of Sweden. (2024). *This is civil defence.* Retrieved from https://www.government.se/government-policy/civil-defence/this-is-civil-defence/

Guillaume, M. (2019). *Combating the manipulation of information – a French case.* (Hybrid CoE Strategic Analysis 16). Helsinki: Hybrid CoE. Retrieved from https://www.hybridcoe.fi/wp-content/uploads/2020/07/HybridCoE_SA_16_manipulation-of-information_.pdf

Hall, H. (2017). The new voice of America: Countering Foreign Propaganda and Disinformation Act.

Hjort, M (2004) *"Nationens livsfråga"* : propaganda och upplysning i försvarets tjänst 1944-1963. Santérus Jeangène Vilmer, J., Escorcia, A., Guillaume, M., & Herrera, J. (2018). Information Manipulation: A Challenge for Our Democracies. Retrieved from https://www.diplomatie.gouv.fr/IMG/pdf/information_manipulation_rvb_cle838736.pdf

Keršanskas, V. (2020). DETERRENCE: Proposing a more strategic approach to countering hybrid threats. *Hybrid CoE Paper 2.* Retrieved from https://www.hybridcoe.fi/wp-content/uploads/2020/07/Deterrence_public.pdf

LaForge, G. (2020). *Sweden Defends its Election Against Disinformation, 2016–2018.* The Princeton University Liechtenstein Institute for Self-Determination. Retrieved from https://successfulsocieties.princeton.edu/sites/g/files/toruqf5601/files/GL_Swedena_Election_FINAL12_23_20_V1_0.pdf

von der Leyen, U. (2024) *Speech at the Democracy Summit in Copenhagen, Denmark,* 14 May 2024. Retrieved from https://download.ursula2024.eu/Speech_Copenhagen_14_05.pdf

Medieakademin. (2023). *Förtroendebarometern 2023*. Microsoft's digital Threat Analysis Center (DTAC). (2023). *DRAFT WHITE PAPER: An attribution model for influence operations.* Retrieved from https://blogs.microsoft.com/wp-content/uploads/prod/sites/5/2023/02/DTAC-Attribution-Framework.pdf

Myers, S. & Frenkel, S. (2023, June 19). G.O.P. Targets Researchers Who Study Disinformation Ahead of 2024 Election. *The New York Times*. Retrieved from https://www.nytimes.com/2023/06/19/technology/gop-disinformation-researchers-2024-election.html

Ministry of Defence (2023). *New assignment and increased funding to Psychological Defence Agency.* Retrieved from https://www.government.se/press-releases/2023/08/new-assignment-and-increased-funding-to-psychological-defence-agency/

NATO. (2020). NATO's approach to countering disinformation: a focus on COVID-19. Retrieved from https://www.NATO.int/cps/en/NATOhq/177273.htm#intro

NATO. (2024). *Countering hybrid threats*. Retrieved from https://www.NATO.int/cps/en/NATOhq/topics_156338.htm

Nakashima, E. (2019, February 27). US Cyber Command Operation Disrupted Internet Access of Russian Troll Factory on Day of 2018 Midterms. *The Washington Post*. Retrieved from https://www.washingtonpost.com/world/national-security/us-cyber-command-operation-disrupted-internet-access-of-russian-troll-factory-on-day-of-2018-midterms/2019/02/26/1827fc9e-36d6-11e9-af5b-b51b7ff322e9_story.html

Newman, H. (2022). Foreign information manipulation and interference defence standards: Test for rapid adoption of the common language and framework 'DISARM'. *Hybrid CoE Research Report 7*. Retrieved from https://www.hybridcoe.fi/wp-content/uploads/2022/11/20221129_Hybrid_CoE_Research_Report_7_Disarm_WEB.pdf
Nilsson, N., Weissmann, M., & Palmertz, B. (2024, forthcoming). Hybrid Threats and the Intelligence Community: Priming for a Volatile Age. *International Journal of Intelligence and CounterIntelligence.*

Pamment, J., & Agardh-Twetman, H. (2019). Can there be a deterrence strategy for influence operations? J*ournal of Information Warfare, 18*(3), Article 123-135.

Pamment, J. (2020a). *The EU Code of Practice on Disinformation: Briefing Note for the New EU Commission*. Carnegie Endowment for International Peace

Pamment, J. (2020b). *The EU's Role in Fighting Disinformation: An EU disinformation framework (Part 2).* Washington DC: Carnegie Endowment for International Peace

Pamment, J. (2020c). *The EU's Role in Fighting Disinformation: Developing Policy Interventions for the 2020s.* Carnegie Endowment for International Peace

Pamment, J. (2021) *RESIST 2*. London: Government Communication Service

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

Pamment, J. (2022b) How the Kremlin circumvented the EU sanctions on Russian state media in the first weeks of the illegal invasion of Ukraine. Journal of Place Branding & Public Diplomacy

Pamment, J. & Ahonen, A. (2023). *The ethics of outsourcing information conflict: Outlining the responsibilities of government funders to their civil society partners.* Riga: NATO Strategic Communication Centre of Excellence

Pamment, J., Falkheimer, J., & Isaksson, E. (2023). *Malign foreign interference and information influence on video game platforms: Understanding the adversarial playbook.* Myndigheten för psykologiskt försvar. Pamment, J. & Lindvall Kimber, A. (2021) *Fact-checking and debunking: a best practice guide to dealing with disinformation.* Riga: NATO Strategic Communication Centre of Excellence.

Pamment, J., Nothhaft, H., Agardh-Twetman, H., & Fjällhed, A. (2018). *Countering Information Influence Activities: The State of the Art.* Swedish Civil Contingencies Agency (MSB). Stockholm: MSB. Retrieved from https://www.msb.se/sv/publikationer/countering-information-influence-activities–the-state-of-the-art-research-report/

Pamment, J. & Palmertz, B. (2023). Deterrence by Denial and Resilience Building, in Arcos, R., Chiru, I., & Ivan, C. (Ed) *Routledge Handbook of Disinformation and National Security.*

Pamment, J. & Smith, V. (2022) *Attributing Influence Operations: toward a community framework*. Riga: NATO Strategic Communication Centre of Excellence & EU-NATO Hybrid Centre of Excellence

Petersson, O. (2018). *Medborgarna och det psykologiska försvaret. Myndigheten för samhällsskydd och beredskap,* ISBN: 978-91-7383-848-1. Retrieved from https://www.msb.se/sv/publikationer/medborgarna-och-det-psykologiska-forsvaret-studie/

Prime Minister's Office. (2022). *The Government appoints Henrik Landerholm as National Security Adviser.* Retrieved from https://www.government.se/press-releases/2022/11/the-government-appoints-henrik-landerholm-as-national-security-adviser/

Prime Ministers Office. (2023). *Pressträff om Sveriges säkerhet.* Retrieved from https://www.regeringen.se/pressmeddelanden/2023/01/presstraff-om-sveriges-sakerhet/

Prop. 2014/15:109. *Försvarspolitisk inriktning – Sveriges försvar 2016-2020.* Retrieved from https://www.riksdagen.se/sv/dokument-och-lagar/dokument/proposition/forsvarspolitisk-inriktning---sveriges-forsvar_H203109/html/

Prop. 2016/2017:1. *Budgetpropositionen för 2017.* Retrieved from https://www.regeringen.se/contentassets/e926a751d9eb4c978c4d892c659ebc8e/budgetpropositionen-for-2017-hela-dokumentet-prop/

Psychological Defence Agency (MPF) 2023.56. *Struktur för effektiv samverkan för det psykologiska försvaret.* Retrieved from https://www.MPF.se/assets/uploads/2023/06/Slutredovisning_struktur-for-effektiv-samverkan-for-det-psykologiska-forsvaret-1.pdf

Psychological Defence Agency (MPF). (2022). *Mission.* Retrieved from: https://www.MPF.se/en/mission/

Rankin, J. (2017, November 13). Catalan independence: EU experts detect rise in pro-Kremlin false claims. *The Guardian.* Retrieved from https://www.theguardian.com/world/2017/nov/13/catalan-independence-eu-experts-detect-rise-in-pro-kremlin-false-claims

Rossbach, N. (2017). *Fighting Propaganda: The Swedish Experience of Psychological Warfare and Sweden's Psychological Defence, 1940-1960.* Axel and Margaret Ax:son Johnson Foundation.

Ranstorp, M. & Ahlerup, L. (2023). *LVU-kampanjen: Desinformation, konspirationsteorier, och kopplingarna mellan det inhemska och det internationella i relation till informationspåverkan från icke-statliga aktörer.* Retrieved from https://www.fhs.se/download/18.32d29dd2187bd01d5e455265/1682576119173/LVU-kampanjen.pdf

Schelling, T. (1966.) *Arms and Influence,* New Haven: Yale University Press.

SOU (Government Official Inquiries). (1953:27). Psykologisk försvar.

SOU (Government Official Inquiries). (2020:29). En ny myndighet för att stärka det psykologiska försvaret. Retrieved from https://www.regeringen.se/rattsliga-dokument/statens-offentliga-utredningar/2020/05/sou-202029/

SOU (Government Official Inquiries). (2021:25). Struktur för ökad motståndskraft. Retrieved from: https://www.regeringen.se/rattsliga-dokument/statens-offentliga-utredningar/2021/04/sou-202125/

Swedish Armed Forces. (n.d.). Svenskt psykförsvar i backspegeln . Retrieved from https://www.forsvarsmakten.se/sv/information-och-fakta/var-historia/artiklar/svenskt-psykforsvar-i-backspegeln/

SFS 2008:1002. Instruktion för Myndigheten för samhällsskydd och beredskap.

SFS 1954:628.

SFS 1985:476. Instruktion för styrelsen för psykologiskt försvar.

SFS 2002:518. Instruktion för krisberedskapsmyndigheten.

SFS 2007:856. Instruktion för Krisberedskapsmyndigheten.

SFS 2015:152. Instruktion för Svenska institutet.

SFS 2021:936. Instruktion för Myndigheten för psykologiskt försvar.

SFS 2022:120. Översyn av lagen om signalspaning i försvarsunderrättelseverksamhet.

Slick, S., Busby, J., & Nguyen, K. (2023). *2022 Public Attitudes on US Intelligence.* The Chicago Council on Global Affairs. Retrieved from https://globalaffairs.org/research/public-opinion-survey/2022-public-attitudes-us-intelligence

Swedish Civil Contingencies Agency (MSB). (2018). *Countering information influence activities – A handbook for communicators.* Retrieved from https://www.msb.se/siteassets/dokument/publikationer/english-publications/countering-information-influence-activities---a-handbook-for-communicators.pdf

Swedish Civil Contingencies Agency (MSB) (2018). *If Crisis or War Comes.* Retrieved from https://www.msb.se/en/rad-till-privatpersoner/the-brochure-if-crisis-or-war-comes/

Sörensen, S. & Pamment, J. (2023) *Operationalising the Framework for Evaluating Capability against Information Influence Operations: A Case Study of the Psychological Defence Agency's Courses.* Riga: NATO Strategic Communication Centre of Excellence

The European Union Agency for Cybersecurity (ENISA). (2022). *Foreign Information Manipulation and Interference (FIMI) and Cybersecurity- Threat Landscape.* Retrieved from file:///Users/el2105is/Downloads/Foreign%20 Information%20Manipulation%20and%20Interference%20(FIMI)%20and%20 Cybersecurity%20-%20Threat%20Landscape%20(2).pdf

The Swedish Agency for Public Management 2017:5. *Myndigheternas arbete med psykologiskt försvar.* Retrieved from https://www.statskontoret.se/publicerat/publikationer/publikationer-2017/myndigheternas-arbete-med-psykologiskt-forsvar/

The Swedish Security Police. (2023). *Försämrat säkerhetsläge när bilden av Sverige förändras.* Retrieved from https://www.sakerhetspolisen.se/ovriga-sidor/nyheter/nyheter/2023-07-26-forsamrat-sakerhetslage-nar-bilden-av-sverige-forandras.html

Tubin, E. (2003). *Förfäras ej.* Styrelsen för psykologiskt försvar. Retrieved from https://www.forsvarsmakten.se/globalassets/forfaras-ej.pdf

World Economic Forum. (2016). *The Global Risks Report 2016.* Retrieved from https://www3.weforum.org/docs/GRR/WEF_GRR16.pdf

World Economic Forum. (2024). *Global Risks 2024: Disinformation Tops Global Risks 2024 as Environmental Threats Intensify.* Retrieved from https://www.weforum.org/press/2024/01/global-risks-report-2024-press-release/

Zerfass, A., Verčič, D., Nothhaft., H., & Werder, K. (2018). Strategic Communication: Defining the Field and its Contribution to Research and Practice. *International Journal of Strategic Communication,* 12:4, 487-505, DOI: 10.1080/1553118X.2018.1493485

Ördén, H. & Pamment, J. (2021). What is so Foreign about Foreign Influence Operations? Washington DC: *Carnegie Endowment for International Peace*

Annex 1. Psychological defence responsibilities over time

Annex 1. Psychological defence responsibilities over time

Organisation	Peacetime Responsibilities	Wartime Responsibilities
SIS[12] **1940–1945**	• Inform, examine, map, and control Swedish public opinion. • Counter foreign propaganda.	• The responsibilities assigned to SIS pertained to measures taken both in peacetime and during war.
BN[13] **1954–1985**	• Contingency planning for psychological defence. • Prepare the National Information Center (UC), the psychological defence's wartime organization. • Funding and research. • Study the development of Swedish opinion and foreign propaganda directed at Swedish opinion. • Monitor Swedish information activities relevant to psychological defence preparedness. • Collaborate with other bodies for these pursuits.	• No wartime responsibilities.
UC[14] **1954–1985**	• No peacetime responsibilities.	• Coordinate public information. • Preserve and strengthen the population's willingness to defend itself and its spirit of resistance. • Monitor public sentiment. • Analyse foreign propaganda. • Counter psychological warfare directed against the Swedish people.
TUN[15] **1961–1985**	• Support and coordinate information on security policy and the Swedish total defence to strengthen the population's willingness to defend.	• No wartime responsibilities.
SPF[16] **1985–2008**	• Lead and coordinate planning of psychological defence, coordinating wartime organisation, wartime planning, and other preparedness arrangements within the function. • Spread knowledge about security policy and total defence. • Promote and coordinate information from other authorities in these fields.	• Maintain and strengthening the population's willingness to defend and its spirit of resistance. • Promote free news dissemination. • Counter psychological warfare • Provide recommendations to the government for measures that could reduce an attacker's psychological resilience.

[12] SFS 1940:60

[13] SOU 1953:27; SFS 1054:628; SFS 1065:681; SFS 1980:601

[14] SOU 1953:27; Government Meeting Records June 7, 1956, case 57 in SOU 2020:29, p. 48

[15] SOU 1961:18; SFS 1962:310; SFS 1975: 892; 1983:482

[16] SFS 1985:476; Prop. 1984/85:160

Organisation	Peacetime Responsibilities	Wartime Responsibilities
KBM[17] **2002–2008**	• Coordinate efforts related to society's preparedness for crisis and civil defence. • Raising awareness and enhancing crisis management capabilities through education and training. • Managing the Rakel communication system. • Develop crisis communication methods. • Conduct external monitoring and analyses of global developments. • Provide situational reports to the government during crises.'	• Provide support and information to the Swedish Armed Forces regarding civil defence readiness.
MSB[18] **2009–2021**	• Have the capability to identify and counteract information influence and the dissemination of misleading information *within its areas of responsibility*. • Contribute to the preparedness of other supervisory authorities and relevant stakeholders in this area through knowledge dissemination and support for collaboration. • Support media companies' contingency planning. • Provide secondment for civil servants to NATO's Center for Strategic Communication in Riga (Since 2016). • Have the capability to identify and counteract information influence and the dissemination of misleading information *directed towards Sweden* (Since 2017). • Provide secondment for civil servants to the European External Action Service (EEAS) (Since 2019).	• The responsibilities assigned to MSB pertained to measures taken before, during, and after accidents, crises, war, or in the threat of war.
MPF[19] **2022–**	• Lead the coordination and development of government and other actors' activities in Sweden's psychological defence. • Contribute to strengthening the population's resilience. • Identify, analyse, and provide support in countering malign information influence and misleading information targeting Sweden or Swedish interests. • Contribute to public awareness, training, research, and collaboration among stakeholders in psychological defence. • Support media companies in identifying, analysing, and countering malign information influence when requested. • Provide the government with information for psychological defence development. • Promptly inform the government about any malicious information influence and the dissemination of misleading information that could impact Sweden's security. • Provide secondment for civil servants to the European External Action Service (EEAS) and the NATO Center of Excellence	• Continue peacetime responsibilities with an emphasis on wartime activities and operations. • Support the government and propose actions to diminish a potential aggressor's capability and intent to attack.

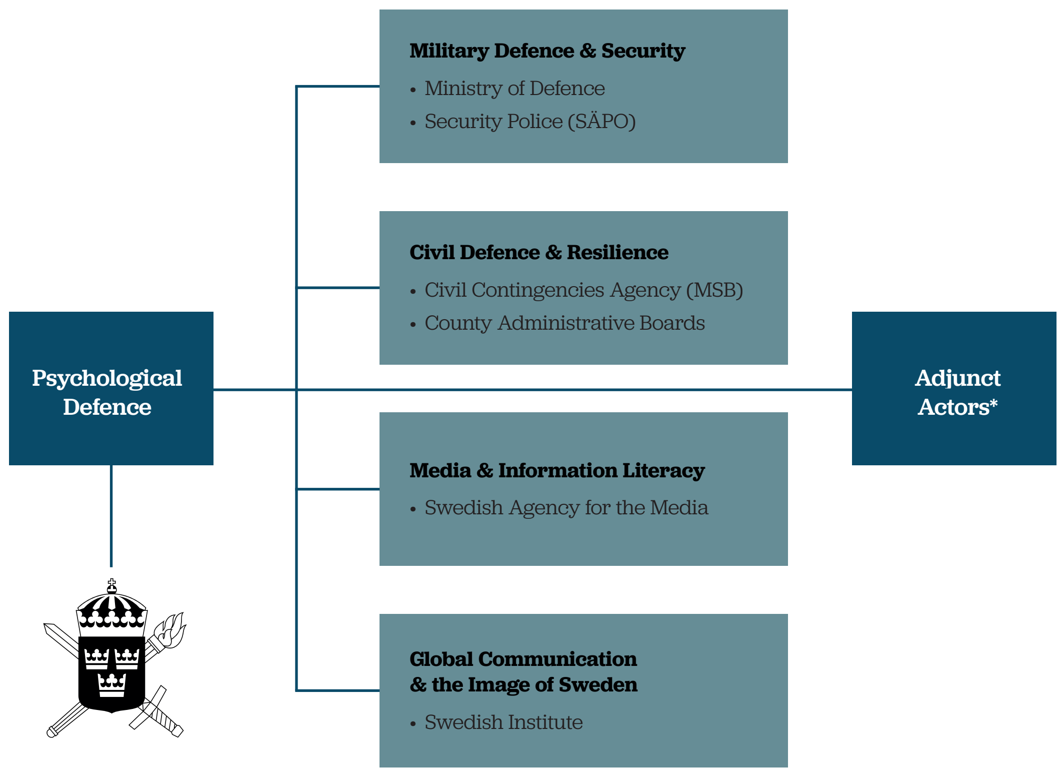
[17] SFS 2002:518; SFS 2007:856
[18] SFS 2008:1002; SFS 2010:1062; Ju2016/06352/SSK; Ju2016/07731/SSK

[19] SOU 2020:29; SFS 2021:936

Annex 2. Psychological defence cooperation structure

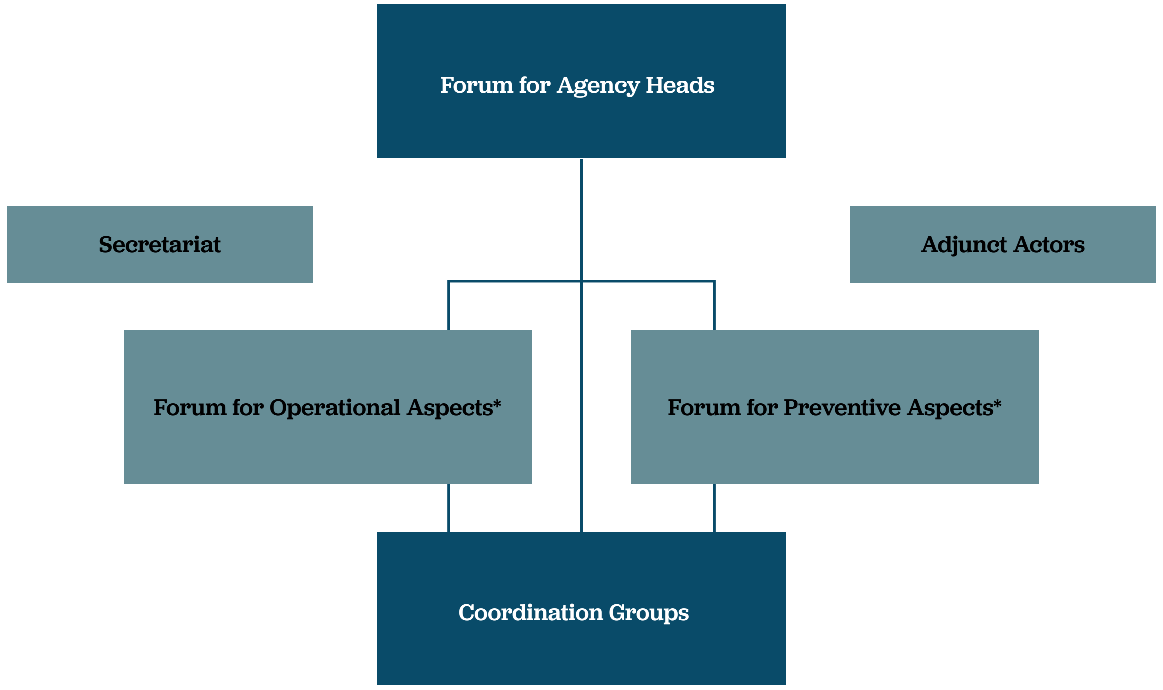
Annex 2. Psychological defence cooperation structure

Figure 1: Areas for psychological defence cooperation & participating organisations (2024)


Psychological Defence
Military Defence & Security
• Ministry of Defence
• Security Police (SÄPO)
Civil Defence & Resilience
• Civil Contingencies Agency (MSB)
• County Administrative Boards
Media & Information Literacy
• Swedish Agency for the Media
Global Communication & the Image of Sweden
• Swedish Institute
Adjunct Actors*

**The collaboration structure is designed to allow for the inclusion of other authorities or actors when required by a certain situation.*

Figure 2: Collaboration Council for Psychological Defence

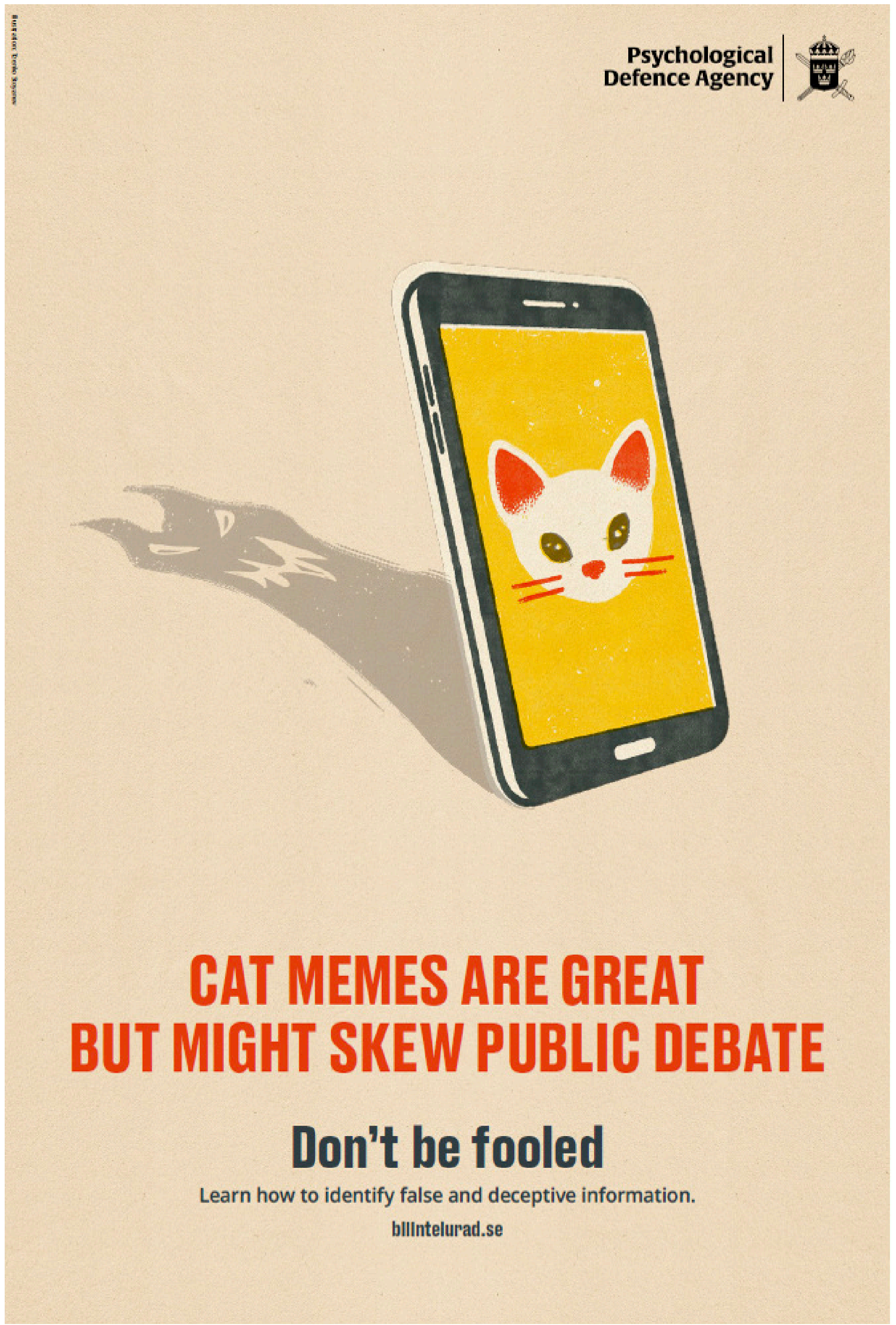


*The forum for operational aspects (*Forum för operativa frågor*) aims to increase collective capability for coordinated operational action. This includes ensuring that the collaborating actors have sufficient knowledge about the nature of threats, societal vulnerabilities, tasks of other relevant actors, capabilities etc. It meets as needed or at least twice a year, represented by operational managers or equivalent from the collaborating actors.

*The forum for preventive aspects (*Forum för förebyggande frågor*) aims to facilitate collaboration among participating actors by focusing on preventive measures, knowledge development, and long-term capability building within psychological defence. It meets as needed or at least twice a year represented with executive-level representation.

Annex 3: Don’t Get Fooled! Bli inte Lurad!

Annex 3. Don’t Get Fooled! Bli inte Lurad!



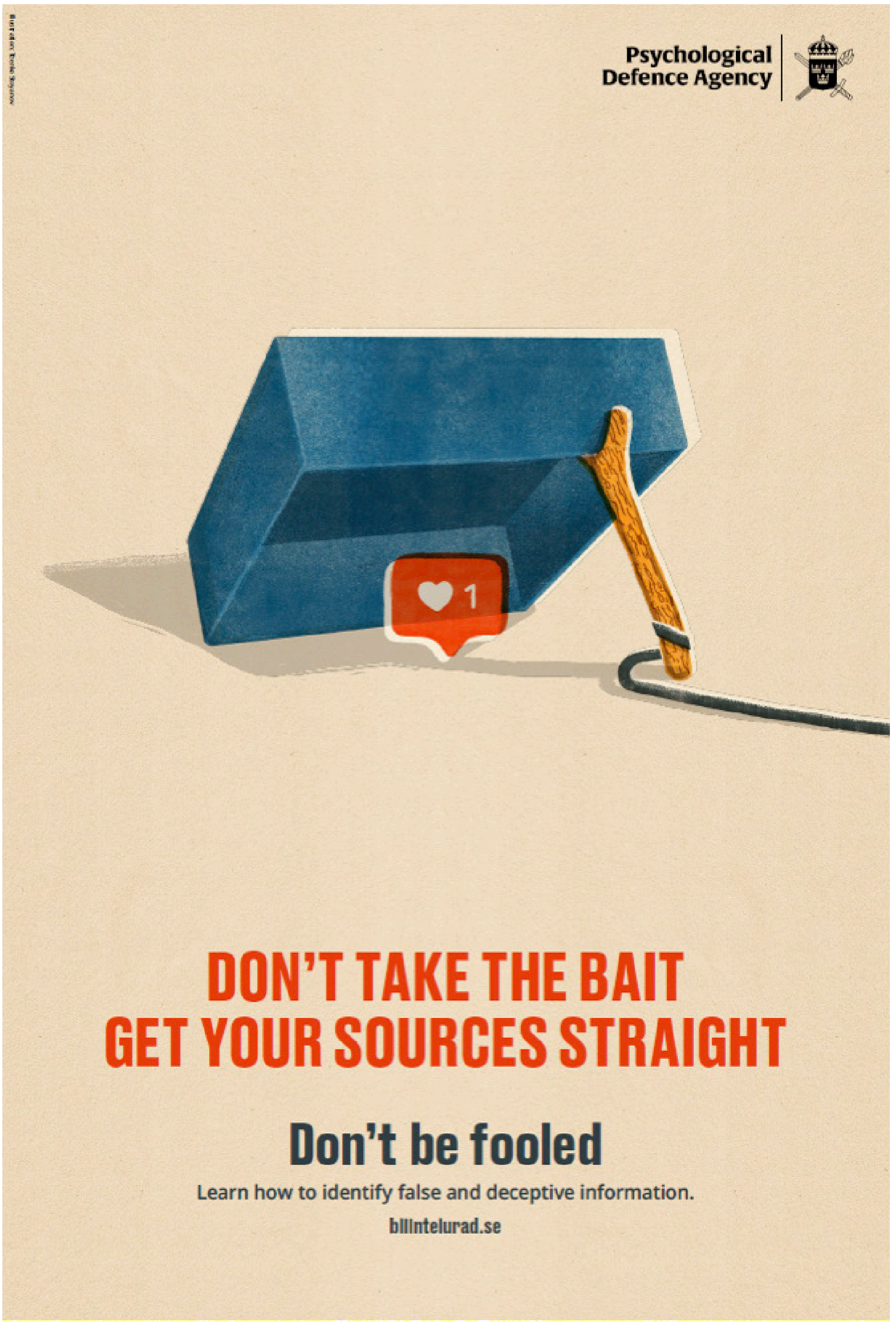
Psychological Defence Agency

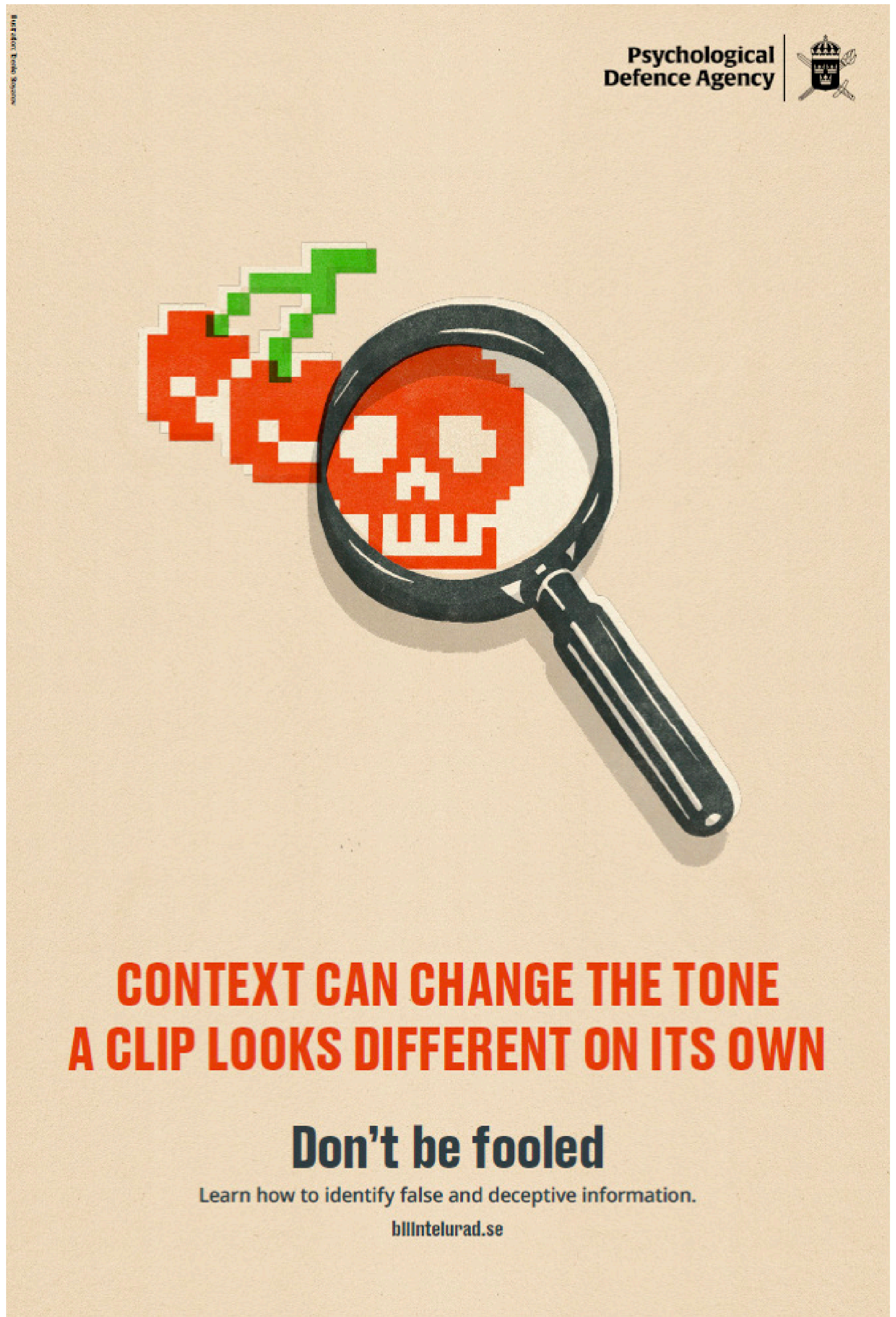
CAT MEMES ARE GREAT BUT MIGHT SKEW PUBLIC DEBATE

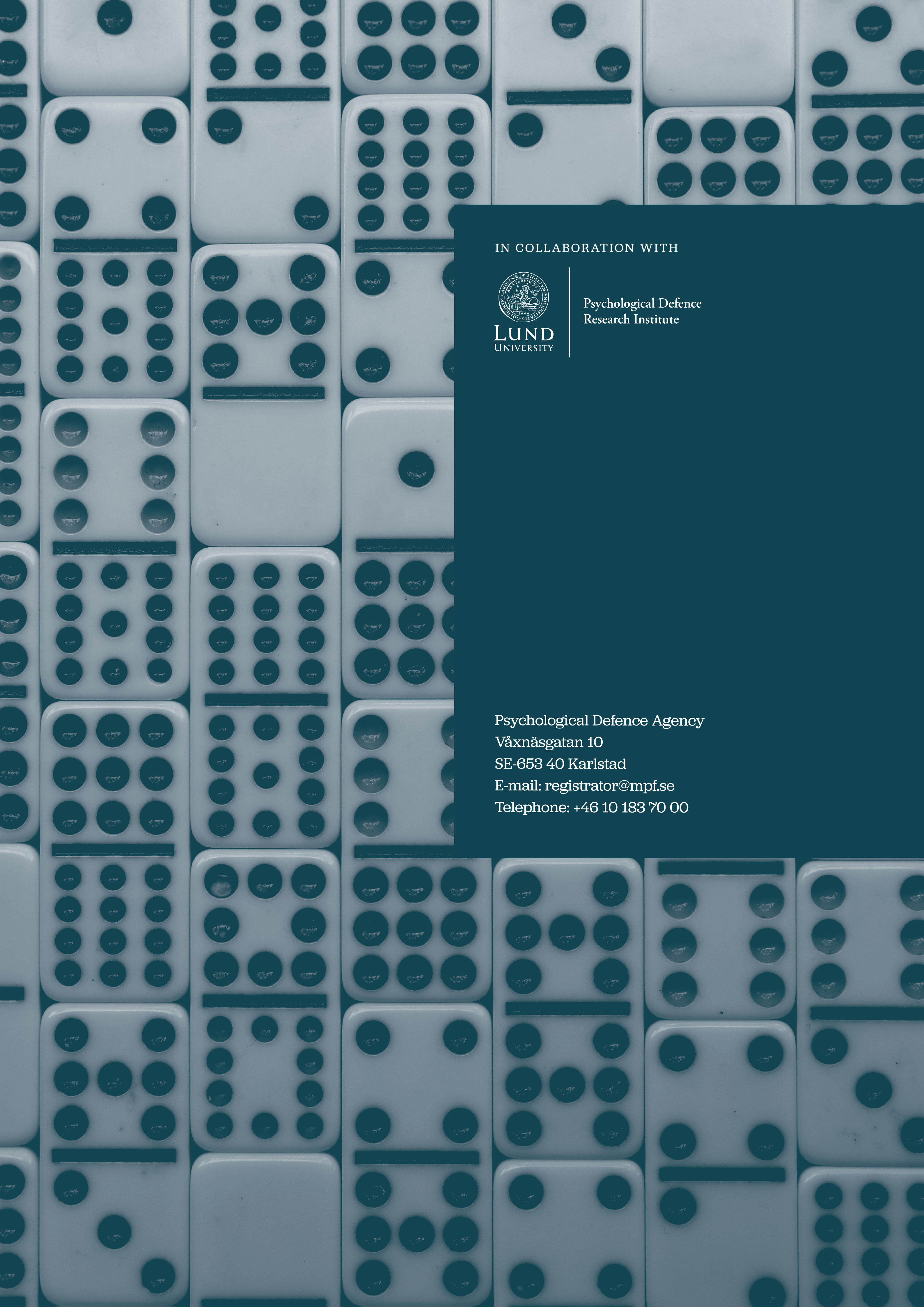
Don’t be fooled

Learn how to identify false and deceptive information.

bliintelurad.se


Psychological Defence Agency
1
DON'T TAKE THE BAIT
GET YOUR SOURCES STRAIGHT
Don't be fooled
Learn how to identify false and deceptive information.
bliintelurad.se


Psychological Defence Agency
CONTEXT CAN CHANGE THE TONE
A CLIP LOOKS DIFFERENT ON ITS OWN
Don't be fooled
Learn how to identify false and deceptive information.
bliintelurad.se



IN COLLABORATION WITH

LUND
UNIVERSITY

Psychological Defence
Research Institute

Psychological Defence Agency
Våxnäsgatan 10
SE-653 40 Karlstad
E-mail: registrator@mpf.se
Telephone: +46 10 183 70 00