

Hybrid Threats, Cognitive Warfare, and Psychological Defence

A PRACTITIONERS' TOOLBOX FOR INTELLIGENCE ANALYSIS
AND RESILIENCE-BUILDING

Docent Dr. Mikael Weissmann (editor)

Associate Professor
Swedish Defence University

Docent Dr. Niklas Nilsson

Associate Professor
Swedish Defence University

Björn Palmertz

Senior Advisor
Psychological Defence Research Institute
Lund University

Dr. Johan Engvall

Deputy Research Director
Swedish Defence Research Agency (FOI)



**HYBRID
THREATS
RESEARCH
GROUP**

HYBRID THREATS, COGNITIVE WARFARE, AND PSYCHOLOGICAL DEFENCE

A PRACTITIONERS' TOOLBOX FOR INTELLIGENCE ANALYSIS AND
RESILIENCE-BUILDING

Docent Dr. Mikael Weissmann (editor)
Department of Systems Science for Defence and Security
Swedish Defence University

Docent Dr. Niklas Nilsson
Department of War Studies and the Centre for Total Defence and Societal
Security (CTSS)
Swedish Defence University

Björn Palmertz
Lund University Psychological Defence Research Institute
Lund University

Dr. Johan Engvall
Swedish Defence Research Agency (FOI)



<https://www.hybridthreatsresearch.com/>

Docent Dr. Mikael Weissmann, Department of Systems Science for Defence and Security, Swedish Defence University.

<https://orcid.org/0000-0001-5426-8238>

Docent Dr. Niklas Nilsson, Department of War Studies and the Centre for Total Defence and Societal Security (CTSS), Swedish Defence University.

<https://orcid.org/0000-0003-3339-3536>

Björn Palmertz, Lund University Psychological Defence Research Institute, Lund University.

Dr. Johan Engvall, Swedish Defence Research Agency (FOI).

Funding was received from the Swedish Psychological Defence Agency and the Swedish Armed Forces (Forskning och Teknik). This toolbox was created as part of a Visiting Scholarship at the European Union Centre in Taiwan, National Taiwan University, Taipei, June–August 2025 funded by a MOFA Taiwan Fellowship.

Publisher: Hybrid Threats Research Group

Year published: 2025

DOI: <https://doi.org/10.5281/zenodo.17763856>

ISBN: 978-91-531-7376-2 (print)

ISBN: 978-91-531-7377-9 (electronic)

Copyright © 2025 by the authors.

Hybrid Threats Research Group

Stockholm

www.hybridthreatsresearch.com



<https://www.hybridthreatsresearch.com/>

The Hybrid Threats Research Group (HTRG) is an interdisciplinary academic initiative focused on advancing the ability to identify, analyse, and respond to hybrid threats in today's highly interconnected world. Our research addresses the multifaceted nature of hybrid threats by blending conventional and unconventional tactics that challenge social, political, and technological resilience.

Our team, comprising experts from fields including political science, strategic communication, war and defence studies, cybersecurity, influence operations, intelligence, and area studies, examines both the inter- and intra-state dimensions of hybrid threats. We work to deepen knowledge of psychological defence mechanisms, such as threat analysis, resilience-building, and the development of operational countermeasure capabilities. This understanding could inform evidence-based policies and practices that enhance preparedness and defence capabilities in complex threat environments. Through our research and international collaboration, we contribute to a body of knowledge that supports government institutions and key societal actors in building capabilities to identify, analyse, and counter hybrid threats.

HTRG Steering Group

Docent Dr. Mikael Weissmann, Senior Lecturer in Systems Science for Defence and Security and an Associate Professor in War Studies, Department of Systems Science for Defence and Security, Swedish Defence University

Docent Dr. Niklas Nilsson, Senior Lecturer and Associate Professor in War Studies, Department of War Studies and the Centre for Total Defence and Societal Security (CTSS), Swedish Defence University

Björn Palmertz, Senior Advisor, Psychological Defence Research Institute (PDRI), Lund University

Dr. Johan Engvall, Deputy Research Director, Swedish Defence Research Agency (FOI)

ABSTRACT

This toolbox consolidates key practitioner takeaways from five publications authored by members of the Hybrid Threats Research Group into a single practitioner’s toolbox for countering hybrid threats and cognitive warfare and for strengthening psychological defence and resilience. The toolbox brings together models developed and published by the group. It links short-term threat–response cycles to long-term resilience and psychological defence, and operationalises national-level psychological defence in a convenient, ready-to-use format.

First, the hybridity blizzard model depicts how the aggressor’s targeting of vulnerabilities interacts with the defender’s responses over time, situating intelligence at the interface of detection and countermeasures with resilience-building. The model also outlines responses to challenges in the contemporary operational environment, highlighting key focus areas for intelligence community actors across analysis, communication, and capability development.

Second, the intelligence analysis interaction (hourglass) model captures three coupled processes – analysis, aggregated, tailored communication, and reception/absorption among societal actors. This model highlights bottlenecks and the need for feedback-rich, whole-of-society practice.

Third, an analytical framework for building resilience and psychological defence countering hybrid threats and foreign influence and interference is outlined. This assess–address–evaluate framework provides a six-dimensional structure, including 1) threat assessment, 2) vulnerability assessments, 2) defence mechanisms, 3) coordination and cooperation, 4) legal/policy framework, and 5) impact and effectiveness. It guides analysis, action, and learning for psychological defence and resilience.

Together, these elements provide practitioners with a practical toolbox to diagnose hybrid activity, design intelligence interactions that resonate well with the recipient (consumers), and strengthen resilience and psychological defence through a coordinated whole-of-society approach.

CONTENTS

- The toolbox 9
- Introduction..... 11
- Tool 1: Hybridity blizzard model for diagnosis and planning 13
 - The role of intelligence and security services 16
- Tool 2: The intelligence analysis interaction (hourglass) model 19
- Tool 3: Building resilience and psychological defence: the assess–address–evaluate model 25
 - Assess, address, and evaluate..... 27
 - The six dimensions of foreign interference 28
 - Assess 28
 - Address 29
 - Evaluate 30
 - Analytical guidebook..... 31
- Conclusion 35
- Reference list..... 37
- Appendix 1: Analytical guidebook 39

FIGURES

- Figure 1: Hybridity blizzard model..... 14
- Figure 2: Complexity of hybrid threats and cognitive warfare..... 15
- Figure 3: The role of intelligence and security services 17
- Figure 4: The intelligence analysis interaction model (hourglass model) 21
- Figure 5: Analytical framework for countering hybrid threats, cognitive warfare and other forms of foreign influence and interference 27
- Figure 6: Analytical guidebook for countering foreign interference 31
- Figure 7: Analytical guidebook - Analyse..... 32
- Figure 8: Analytical guidebook - Address 32
- Figure 9: Analytical guidebook - Evaluate 33

THE TOOLBOX

This toolbox collates a selection of previously published material from the Hybrid Threats Research Group (HTRG) into a single practitioner's toolkit. The authors of this report are the steering group members of the HTRG. The toolbox is based on text and findings from the following publications:

1. Nilsson, N, Weissmann, M., and Palmertz, B (2026) 'Hybrid Threats and the Intelligence Community: Priming for a Volatile Age', *International Journal of Intelligence and CounterIntelligence*, 39(1), pp. 109-131. <https://doi.org/10.1080/08850607.2024.2435265>
2. Weissmann, M. (2025) 'Future Threat Landscapes: The Impact on Intelligence and Security Services', *Security and Defence Quarterly*. 49(1), pp. 40–57. <https://doi.org/10.35467/sdq/197248>
3. Palmertz, B, Weissmann, M., Nilsson, N., and Engvall, J. (2024) *Building Resilience and Psychological Defence: An Analytical Framework for Countering Hybrid Threats and Foreign Influence and Interference*. Lund University Psychological Defence Research Institute, Lund. Available at: <https://fhs.diva-portal.org/smash/record.jsf?pid=diva2%3A1846756> (Accessed: 28 November 2025)
4. Weissmann, M. (2024) 'Framtida hotbilders påverkan för säkerhetstjänsterna', in H. Häggström (ed.) *Framtidens säkerhetstjänst i totalförsvaret*. Swedish Defence University Report Series, Stockholm, pp. 38–67. <https://doi.org/10.62061/OVWF1511>
5. Weissmann, M, Nilsson, N., and Palmertz, B. (2021) 'Moving out of the Blizzard: Towards a Comprehensive Approach to Hybrid Threats and Hybrid Warfare', In M. Weissmann, N. Nilsson, B. Palmertz, and P. Thunholm (eds.) *Hybrid Warfare: Security and Asymmetric Conflict in International Relations*. I.B. Tauris, London, pp. 263–272. <http://doi.org/10.5040/9781788317795.0025>

The views and opinions presented in this publication are those of the authors alone and do not necessarily represent those of the Swedish Defence University, the Swedish Armed Forces, or the Swedish Defence Research Agency.

In the preparation of this toolbox, the editor utilised generative AI and AI-assisted technologies to support the writing process, including to translate the Swedish text. The tools included ChatGPT, Gemini, Grammarly, Google Translate, and DeepL Translate, which were used as support tools and not as a substitute for scholarly judgment. The authors carefully reviewed, edited, and validated the content to ensure its accuracy and integrity and take full responsibility for the final published work.

The toolbox contains limited new findings and text, no new data, and only light harmonisation across sources.

INTRODUCTION

The international security environment has become increasingly contested and unpredictable. The international order is characterised by asymmetric conflicts and great power competition, with countries such as Russia, China, Iran, and North Korea pursuing strategies to achieve national goals by developing and combining unconventional, less resource-intensive means to compete with the West on the global stage. Asymmetric strategies are also utilised by non-state actors, notably ISIS and Hezbollah. Centrally, these strategies increasingly include cognitive warfare – deliberate efforts to target the perception, attention, and trust of individuals and groups to shape their behaviour and erode societal cohesion.

Consequently, security challenges arising from hybrid threats and cognitive warfare, which exploit and combine kinetic and non-kinetic tools ranging from sabotage, influence operations, and cyberattacks to coercive diplomacy and economic dependencies, have emerged on security agendas worldwide. These salient concerns continuously present new challenges for democracies, their armed forces, the broader defence sector, and society as a whole. In the case of cognitive warfare, which operates at the human-domain layer of hybrid threats, the effects of the other tools are amplified by undermining trust in institutions, corrupting information environments, and inducing maladaptive decisions between leaders and the public.¹

While not the only sector impacted, the intelligence community stands at the forefront of identifying and analysing the present security environment's hybrid threats, including cognitive warfare. The intelligence community play a crucial role in coordinating and integrating acquired information among key societal actors affected by these threats or are responsible for countering them. This includes the detection and attribution of cognitive operations, timely warnings about attempts to manipulate public sentiment or decision-making, and support for resilience and psychological defence through actionable assessments and tailored communication.

¹ On cognitive warfare, see for example Backes and Swab (2019), Claverie et al. (2022), Claverie and Du Cluzel (2022), and Hoffman (2025).

The prevalence of hybrid threats and cognitive warfare raises challenges for the intelligence community, whose role is directly related to the nature of these threats. Hybrid threats are complex in that they could target a wide range of societal vulnerabilities across the political, military, economic, social, information, and infrastructure spectrum (PMSII), which might not be susceptible to early detection. The same complexity holds for cognitive warfare, although it specifically targets the cognitive dimension and seeks to exploit social fault lines and biases.

Furthermore, these threats are multifaceted, potentially combining several different resources at the aggressor's disposal into a single strategy for maximum effect. They are also dynamic, implying that they can be adjusted and tailored to target specific vulnerabilities at specific points in time, but can also be altered to target new vulnerabilities as these emerge. Reactive measures by the defender to reduce vulnerabilities in one area may induce neglect or increase vulnerabilities in another, thus opening new avenues for hybrid threats and cognitive warfare.

The remainder of this paper operationalises these challenges using three complementary tools that together form a practical workflow. It starts with diagnosis and planning in Tool 1, the hybridity blizzard model. Next, it explores intelligence production, tailored communication, and absorption in Tool 2, the hourglass model. Finally, it analyses governance and learning at the national level in Tool 3, the assess–address–evaluate (AAE) framework.

Tool 1, the hybridity blizzard model, depicts how the aggressor's targeting of vulnerabilities interacts with the defender's responses over time, situating intelligence work at the interface of detection and countermeasures with resilience-building. It also clarifies the role of the intelligence and security services in this process. The hybridity blizzard model, therefore, anchors the diagnosis step used throughout the report.

Tool 2, the intelligence analysis interaction (hourglass) model, captures three coupled processes – analysis; aggregated, tailored communication; and reception/absorption among societal actors – highlighting bottlenecks and the need for feedback-rich, whole-of-society practices. The hourglass model outlines how intelligence must be aggregated and tailored to ensure absorption among non-traditional consumers.

Tool 3, the AAE framework, provides a six-dimensional structure (threat and vulnerability assessments, defence mechanisms, coordination and cooperation, legal/policy framework, and impact and effectiveness) to guide analysis, action, and learning for psychological defence and resilience. The AAE framework provides an overarching analytical structure into which the blizzard and hourglass are integrated.

TOOL 1: HYBRIDITY BLIZZARD MODEL FOR DIAGNOSIS AND PLANNING²

This tool anchors the diagnosis step used throughout the report. It depicts how the aggressor's targeting of vulnerabilities interacts with the defender's responses over time, situating intelligence work at the interface of detection and countermeasures with resilience-building.

To capture the dynamics of hybrid threats and cognitive warfare, it is essential to include the relationship between the aggressor and the defender from both short- and long-term perspectives. We visualise this relationship in the 'hybridity blizzard model', which schematically outlines the dynamics of the interrelationship between defenders and aggressors in the short and long terms, and how the different time and actor dimensions interact. Both dimensions are important, because hybrid threats are neither one-off events nor activities that can be temporally separated from their context (see Figure 1 below).

The model includes two actors, the defender and the aggressor, together with two temporal dimensions, 'short term' and 'long term'. In the short term, the battle consists of an ongoing mutual interaction between the hybrid threats emanating from the aggressor and the defender's responses as well as countermeasures. It is a continuous and ongoing process with no predetermined beginning or end.

In the longer term, the focus shifts to the defender's vulnerabilities and the resilience built to mitigate them. The aggressor seeks to identify vulnerabilities in order to exploit them. The defender's identification of own 'vulnerabilities' helps build psychological defence and resilience. These efforts logically involve a change in vulnerabilities, which normally decrease; however, any changes made could also theoretically give rise to new vulnerabilities that the aggressor can identify and exploit ('increasing or decreasing vulnerabilities').

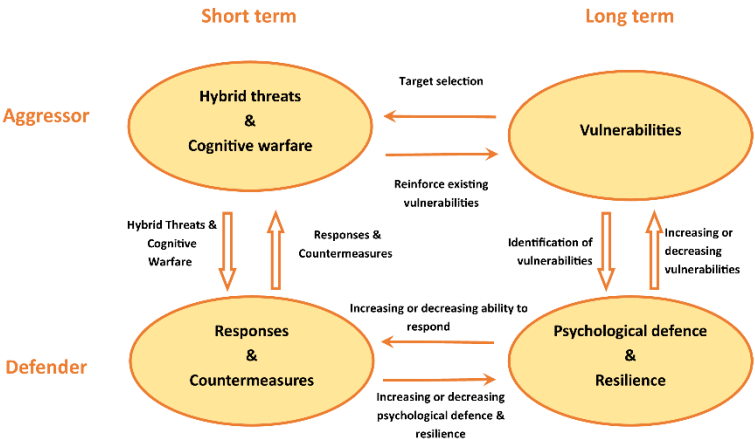
There is also a link between the short- and long-term perspectives.

² This section is an edited adoption from and extension of the model outlined in Weissmann (2024) and Nilsson, Weissmann and Palmertz (2025); also see Weissmann, Nilsson and Palmertz (2021).

When the aggressor designs a hybrid method, the vulnerabilities it identifies are a crucial component of the ‘target selection’. Furthermore, by targeting weaknesses, all else being equal, existing vulnerabilities will increase (and then likely become the focus of new attacks, etc.).

On the defender’s side, there is also a relationship between short-term responses and countermeasures, on the one hand, and building longer-term resilience and psychological defence, on the other. Existing psychological defence and resilience affects the defender’s ability to respond to and implement countermeasures against different attacks and threats (‘increasing or decreasing ability to respond’). In turn, the responses and countermeasures increase or decrease defender resilience. In summary, there is a back-and-forth process between the long and short terms on both sides.

Figure 1: Hybridity blizzard model



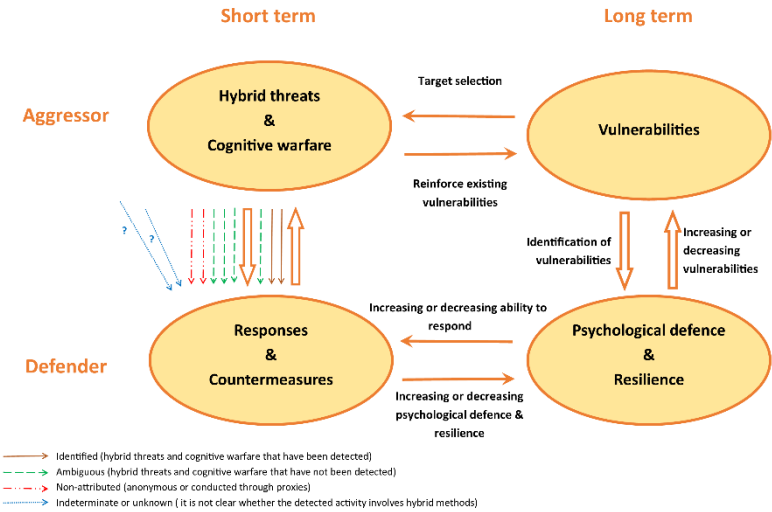
Source: Authors’ model, developed from Weissmann, Nilsson, and Palmertz (2021); Nilsson, Weissmann, and Palmertz (2026).

Hybrid threats and cognitive warfare often emerge and thrive in environments characterised by chaos, confusion, and denial. The image of a blizzard is useful here: the target of hybrid action is constantly and blindly buffeted from all possible and impossible directions by countless micro-attacks that cannot be cleanly separated or localised, preventing the defender from responding and acting effectively (see Figure 2 below).

In principle, many more arrows can be drawn in different parts of Figure 2. The short-term side of the model, where the decisive components best connect to the snowstorm analogy, is the most chaotic. First, threats directed at the defender cannot always be identified; they remain ambiguous, often unattributed, and sometimes even indeterminate or unknown to the defender. Second, there is a non-trivial risk of identifying false positive hybrid threats and cognitive warfare measures.

This is not only a problem in its own right ('crying wolf'); it can itself be a deliberate component of a broader strategy. For instance, is the target of observation someone's proxy, or is the 'proxy' acting independently, outside a larger strategy? Are the problems detected in the power grid or financial infrastructure manifestations of hybrid threats, or are they simply glitches? Is the perceived threat to military medical services or food supply a hybrid threat, or merely a 'regular' hazard with no actor behind it?

Figure 2: Complexity of hybrid threats and cognitive warfare



Source: Authors' model, developed from Weissmann, Nilsson, and Palmertz (2021); Nilsson, Weissmann, and Palmertz (2026).

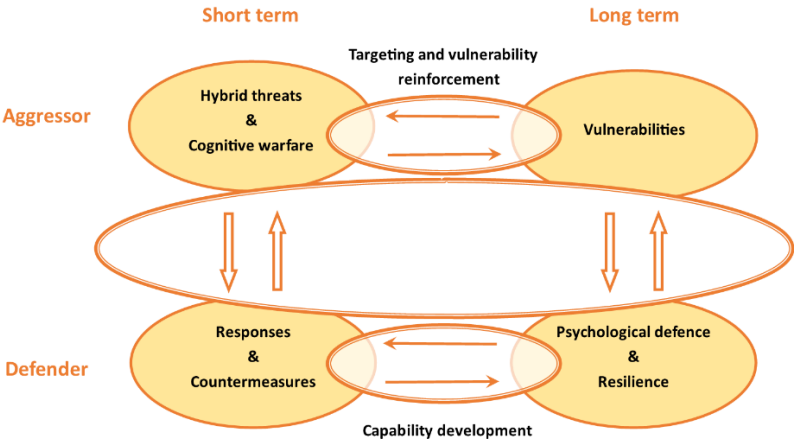
THE ROLE OF INTELLIGENCE AND SECURITY SERVICES

For intelligence and security services, the challenges are particularly concentrated at the intersections between the elements in the hybrid blizzard model (see Figures 2 and 3). At these intersections between aggressor and defender, the intelligence community's ability to identify and comprehensively understand the dynamics of the operational environment is key to defence-building capabilities and the ability to influence threat actors in different domains. In other words, the model depicts the preconditions for intelligence success or failure in the detection and response to hybrid threats and cognitive warfare as being located along the interface of short- and long-term interactions between the aggressor and defender.

The temporal perspective also highlights a crucial role for the intelligence community in the internal process of the defender, where capability development takes place in the relationship between short-term responses and countermeasures, on the one hand, and building longer-term resilience, on the other. At the same time, the aggressor is expected to engage in targeting and reinforcing vulnerability. However, this is not our focus, as this process is internal to the aggressor. These three areas, which represent salient challenges for the intelligence community in relation to hybrid threats are highlighted in yellow in Figure 3 (see below).

In summary, the challenges for intelligence community actors are concentrated in three distinct processes. The first is **intelligence analysis, aggregation, and warning intelligence**. This process is located at the intersection between the aggressor and the defender, where the need emerges to identify and analyse the threats and vulnerabilities present in the operational environment. The second is **the need for intelligence communication and dissemination**, which refers to how intelligence community actors successfully channel their analyses and recommendations to relevant key societal actors responsible for countermeasures and resilience building. The third challenge concerns **responses, countermeasures, resilience-building, and capability development**, constituting a whole-of-society approach to countering hybrid threats and cognitive warfare. The second challenge is addressed by the hourglass model and the third challenge is addressed by the AAE framework.

Figure 3: The role of intelligence and security services



Source: Authors' model, developed from Weissmann (2024); Nilsson, Weissmann, and Palmertz (2026).

TOOL 2: THE INTELLIGENCE ANALYSIS INTERACTION (HOURGLASS) MODEL³

The intelligence analysis interaction model, or the hourglass model, summarises the three critical processes of intelligence work in relation to the hybrid threats and cognitive warfare identified above. The model visualises the links between intelligence analysis, aggregation, and intelligence communication tailored to a wide range of key societal actors as well as the implementation of intelligence in a whole-of-society approach to countering hybrid threats. It also outlines the need to aggregate and tailor intelligence to secure absorption among consumers using non-traditional consumers of intelligence. (See Figure 4 below.)

Thus, the model addresses one of the most prevalent challenges facing the intelligence community in the current security environment: the provision of warning intelligence, intelligence dissemination, and interactions with other key societal actors. The hourglass model presents an understanding of the critical processes in the intelligence community's identification and aggregated analysis of hybrid threats and cognitive warfare, its dissemination of these threats to other key societal actors, and the reception and feedback from these actors, which constitute a co-production of knowledge essential in a whole-of-society approach to countering hybrid threats.

Building societal resilience in the face of widely defined hybrid threats and cognitive warfare requires an equally comprehensive societal response the 'whole-of-society' approach. Several layers of this concept are particularly pertinent in the discussion of hybrid threats and cognitive warfare. Governments and relevant government agencies are primarily responsible for countering and preventing the societal impact of antagonistic threats. Depending on the type of threat concerned, relevant agencies may include military, police authorities, or emergency management agencies, among others. However, given the composite and synergistic nature of hybrid threats, government responses require a

³ This section incorporates and adapts texts from Nilsson, Weissmann, and Palmertz (2025).

purposeful fusion of a wide variety of functions beyond the security apparatus, including those of local government, educational institutions, healthcare, energy, and transportation. The aim is to integrate state responses through a whole-of-government approach, which requires a degree of horizontal organisation to avoid stovepipes in information sharing and decision-making.

A whole-of-society approach goes beyond the confines of government to include and assign responsibilities to other important societal actors, including civil society and the private sector. A key feature of this approach is the development of productive interactions and partnerships between the government, the general public and private actors, with the aim of establishing awareness, collaboration, and preparation as components of building resilience.⁴

The hourglass model is ideal for understanding the mechanism of intelligence analysis interaction. It can also be used as a model representation of a single interaction between an intelligence community actor and a receiving societal actor (consumer). Actual practice consists of numerous interactions, or hourglasses, each with its own dynamics. This is the case when considering the interaction between the range of intelligence actors, both governmental and non-governmental, and the variety of societal actors across all dimensions of the state, public, and private spheres. The model also represents the exchange between particular intelligence actors and key societal actors in receipt of their aggregated analyses.

The intelligence analysis interaction model visualises three critical processes in the interaction between intelligence community actors and key societal actors. The successful execution of these processes is considered crucial for fulfilling the intelligence community's potential to forge a whole-of-society approach to counter hybrid threats. The processes are as follows.

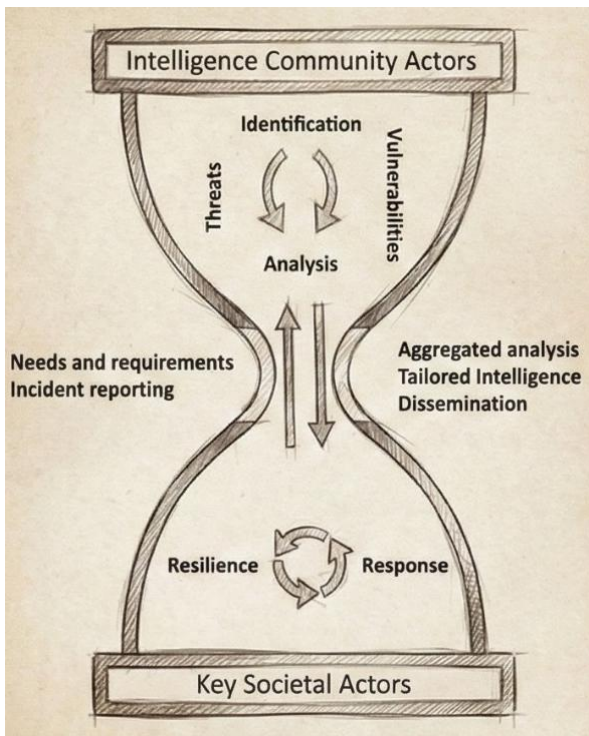
1. **Intelligence analysis** involves intelligence community actors **identifying and analysing antagonistic threats and own vulnerabilities**. This process is represented in the upper part of the hourglass, depicting how the vast flow of information collected by the intelligence community is narrowed down in order to identify threats and vulnerabilities in the haystack of information. These are then analysed and transformed from information into actionable intelligence.
2. **The aggregation and dissemination of intelligence** denote a chokepoint in the interaction between the intelligence community and key societal actors in the receipt of intelligence analyses of threats and vulnerabilities. This zone is not only a bottleneck but also a necessary conduit for the ability to optimise policies and countermeasures in response to hybrid threats that are informed

⁴ Ivan, Chiru, and Arcos (2021).

by the best possible intelligence-based knowledge. Two components are critical for optimal communication of intelligence: **aggregated analysis** and **tailored dissemination**. Just as aggregated data are needed to produce good intelligence analyses, aggregated analysis is required to produce the best possible assessment of the issues in focus or to answer relevant requests for information. Tailored dissemination is required to target the particular requirements of the recipient (consumer). As countermeasures against hybrid threats and cognitive warfare could involve a wide range of societal actors, many of whom are not included in the conventional intelligence consumer base, dissemination may also require adaptation to the recipient's particular characteristics and contextual knowledge.

- 3. The reception and absorption of intelligence** among key societal actors denote an implementation process in which new intelligence broadly feeds into a whole-of-society approach to devise responses to identified and anticipated hybrid threats and cognitive warfare. This is represented by 'capability development' in Figure 3 above.

Figure 4: The intelligence analysis interaction model (hourglass model)



Source: Authors' model, developed from Nilsson, Weissmann, and Palmertz (2026). Image created in Gemini.

Ideally, the three processes of intelligence analysis, dissemination, and reception should be interactive, rather than unidirectional. The intelligence community requires feedback from societal actors on their needs and requirements as well as incident reporting to enhance its ability to identify threats and vulnerabilities and to produce better analyses. Feedback is also an important component for tailoring intelligence dissemination. However, this reciprocal process rarely functions optimally: time constraints, institutional stovepipes, and cultural discrepancies frequently present barriers to systematic feedback from other societal actors to the intelligence community, while channels into the often-insular intelligence community are lacking.

By identifying the three distinct areas, the hourglass model can aid a focused effort in preparing and devising appropriate responses during an escalation of events.

First, by ensuring that the analysis process has access to a wide range of skillsets and sources, it enables comprehensive assessments when numerous sectors and organisational levels of society are targeted simultaneously. Hence, any potential gap between agencies tasked with domestic versus foreign malign interference presents an especially serious weakness.

Second, understanding the need to establish and implement a two-way connection to critical societal actors relevant from a hybrid-threats perspective opens up opportunities for better situational awareness across the societal spectrum. It also facilitates understanding of the realities, professional language, and needs of organisations beyond the traditional national defence establishment, which should be able to find new roles and interpret intelligence briefings.

Third, the analysis process focuses on possibly the most important aspect: how an intelligence community can act as a catalyst for this palette of societal actors to build new skill sets and processes that enable them to act on changing circumstances, alerts, and antagonistic actions. An organisation whose perspective on security has been locked onto crime and natural hazards for years can, in today's deteriorating security environment, be targeted as an attractive vulnerability because it is considered relatively unaware. It may also inhabit a hub position in a critical supply chain or a development cluster, with ramifications that have not been considered. Suddenly, a company or non-defence government entity can be the target of a capable antagonistic foreign state actor because it is perceived as representing a nation within a certain sector, not because it rests within the confines of its normal operations.

Linking back to the hybridity blizzard model (Figures 1 and 2) and the challenges facing the intelligence and security communities in the contemporary operational environment, the 'targeting and vulnerability reinforcement' dimension is

represented by the upper part of the hourglass, where intelligence community actors identify and analyse threats and vulnerabilities. These analyses then need to be channelled to relevant actors to facilitate responses and resilience, which is a necessary input for successful capability development among key societal actors, as shown by the lower part of the hourglass. This dissemination between the analysis level and receivers (consumers) is a critical bottleneck in the intelligence decision and response cycle. Here, sophisticated and timely aggregated analyses channelled through tailored intelligence dissemination are crucial.

The success of the hourglass model depends on **the optimal execution of the three critical processes: intelligence analysis; aggregation and communication of intelligence; and reception and absorption of intelligence among key societal actors.** To counter hybrid threats, building societal resilience requires a whole-of-society approach, in which responsibility is not limited to the government but also includes numerous organisations across the public and private spheres.

Intelligence and security services play a crucial role in identifying vulnerabilities and establishing situational awareness; however, the nature of threats and responses requires a reassessment of what intelligence can and should be shared, how, and for what purpose.

Given the diffuse nature of hybrid threats and cognitive warfare, services must be capable of detecting previously unknown or unanticipated threats and previously unseen combinations of threats. Moreover, these systems should rely on a wide variety of sensors and have the capacity for aggregation, particularly to manage the 'wicked problem' of exponentially increasing data flows and the integration of AI-enabled analysis.⁵

The dissemination of intelligence between the analysis level and consumers is a critical bottleneck in the hourglass model, representing the challenge of appropriately calibrating information flows between the intelligence community and key societal actors. Hybrid threat-warning intelligence today requires a more inclusive and interactive approach to intelligence analysis and aggregation than has traditionally been the case.

In addition, intelligence communication must be more interactive and tailored to different actors, including inexperienced intelligence consumers, and strategies must be developed for interaction with critical sectors. This aligns with recent findings on strategic communication, which suggest that carefully calibrated intelligence disclosures are essential for establishing narrative power, attributing

⁵ Weissmann (2025).

hostile actions, and reinforcing the credibility of government narratives among these broader audiences.⁶

The intelligence community – whether it wants to be or not – has been thrust into the role of an enabler for the development of enhanced resilience and response capabilities across the societal spectrum.

⁶ Nilsson (2025).

TOOL 3: BUILDING RESILIENCE AND PSYCHOLOGICAL DEFENCE: THE ASSESS—ADDRESS—EVALUATE MODEL⁷

The AAE model provides the overarching analytical structure into which the hybrid blizzard and hourglass models can be integrated. It offers a six-dimensional framework that structures analysis, action, and learning related to psychological defence and resilience – needs that have grown significantly in recent years and are likely to continue expanding.

It has become increasingly evident that the need to strengthen resilience and psychological defences against hybrid threats, cognitive warfare, and other forms of foreign influence is greater than ever before. Russia’s full-scale invasion of Ukraine on 24 February 2022 marked a watershed moment, accelerating the trend toward greater volatility and strategic uncertainty, both within Europe and globally. This instability has been further amplified by the growing geopolitical unpredictability associated with the Trump administration in the U.S., which has contributed to heightened international tensions, increased uncertainty regarding U.S. commitments, and wider turbulence in the global security environment.

In parallel, the conflict between Israel and Hamas, broader instability across the Middle East, and rising tensions in the Taiwan Strait and between the United States and China have added additional layers of unpredictability and strain to the international system, fuelling regional escalation risks and complicating the strategic landscape for democratic states. New forms of antagonistic behaviour, including offensive cyber operations, influence campaigns, and other hostile activities by state and non-state actors, have further complicated the security picture.

Against this backdrop, it has become abundantly clear that national resilience and psychological defence capabilities must span the entire conflict spectrum, from peacetime and crisis to high-intensity war. The AAE framework takes this complex threat environment as its starting point. It presents a structured approach to countering hybrid threats, cognitive warfare, and foreign interference by translating broad analytical principles into a practical guide that supports the

⁷ This section incorporates and adapts text from Palmertz *et al.* (2024).

identification and assessment of hostile activities targeting democracies and their national interests.

Analysing hybrid threats and cognitive warfare, as well as any form of foreign interference, is integrated into many analytical areas and encompasses a wide variety of threats. This results in the need for frameworks that can facilitate the collation of various types of information. In addition, owing to the broad nature of how influence can manifest from an adversary against a society, there is a need for a structured and pedagogic approach that can be understood by a broad array of decision-makers. Because hybrid threats and cognitive warfare are often interconnected and simultaneously target multiple aspects of society, there is a need for an analytical framework that simplifies and enables the identification of important interrelated aspects in large and complex volumes of information.

Importantly, the framework must be flexible and, to a certain degree, modular because its application and the resolution needed in the different categories may differ slightly depending on which societal actors will make use of it and at what level they operate. Additionally, one can be certain that capable adversaries continually adapt and develop their means and methodologies.

The framework presented here offers one of several possible approaches to strengthen resilience and psychological defence in democratic states confronted with hybrid threats, cognitive warfare, and other forms of malign foreign influence and interference. For this type of analytical framework to be useful in practice, it must

- account for the diversity of threats and the wide range of domains threatened by adversaries;
- provide a structured approach that supports clear understanding among a broad spectrum of decision-makers;
- simplify the complexity of reality and enable practitioners to identify key interconnections within large volumes of information; and
- allow for flexibility and modularity because its application may differ slightly depending on different categories of threats and the type of practitioners using it.

These four requirements guide the framework presented below.

The framework is intended as a starting point for analysis and is designed for use by both governmental and non-governmental actors. It serves as a platform for examining the multiple dimensions of hybrid threats and malign foreign influence and interference. It also provides tools for comparing and analysing these dimensions, both within and across cases. Furthermore, it forms the basis of a practical analytical guidebook built with modularity in mind, enabling users to

select the components most relevant to their needs and specific questions faced. This finding supports both structured and less-structured qualitative analysis.

ASSESS, ADDRESS, AND EVALUATE

The formation of responses to foreign interference should be seen as a process consisting of three distinct phases:

- 1) establishing situational awareness;
- 2) applying and adapting existing defences and countermeasures, while developing new ones when required; and
- 3) evaluating the overall effectiveness of the system for countering foreign interference.

These phases can be summarised as *assess*, *address*, and *evaluate* (See Figure 5 below).

Figure 5: Analytical framework for countering hybrid threats, cognitive warfare and other forms of foreign influence and interference



Source: Authors’ model, from Palmertz et al. (2024). Image created in Gemini.

Assess refers to the double-sided mapping of external threats, denoting antagonistic actors that seek (or may seek) to exercise malign influence by various means, and the internal vulnerabilities these actors seek (or may seek) to target. It also includes the available defensive mechanisms.

Address denotes the state's existing capabilities for addressing the threats and vulnerabilities identified. This includes existing frameworks for national coordination of these efforts, international cooperation, and existing legal and regulatory frameworks.

Evaluate refers to an integrated analysis, with a view to establishing a holistic understanding of the impact of threats and the effectiveness of capabilities identified above. The evaluation stage should serve as the foundation for informed decisions on whether the state's existing capacity and methods of response require reinforcement, revision, or more fundamental change.

THE SIX DIMENSIONS OF FOREIGN INTERFERENCE

When assessing foreign interference, six key dimensions need to be taken into account: 1. threat assessment, 2. vulnerability assessment, 3. defence mechanisms, 4. coordination and cooperation, 5. legal and policy framework, and 6. impact and effectiveness. The first three belong to the 'assess' phase of the analytical process, that is, the assessment of the threat and one's own vulnerabilities as well as the defence mechanisms that are in place. Dimensions four, coordination and cooperation, and dimension five, legal and policy framework, concern the frame in which the first three dimensions exist. This is the 'address' phase of the process. Finally, dimension six covers the 'evaluate' phase, focusing on the combined impact and effectiveness of the first five.

Assess

Threat assessment concerns the identification and analysis of who the threat actors are – direct or through proxy – and their tactics, techniques, and tools used when attempting to interfere with the country's affairs. Here, the time dimension must be considered because threat levels and patterns of interference may evolve over time. When assessing a threat, there is an inherent need to be forward-looking, asking whether there are any emerging or future threats that the country should anticipate and prepare for.

The second dimension, **vulnerability assessment, concerns the identification and analysis of a country's vulnerability to foreign interference,** that is, the underlying political, social, and economic factors that contribute to the country's vulnerabilities. In this context, it is important to consider each country's governance structure and democratic processes to analyse and understand their impact on vulnerability to foreign interference. Moreover, it is important to include the role and impact of different kinds of societal divisions or issues, as well as societal groups and organisations that are deliberately or unwittingly targeted

and exploited by foreign actors to amplify discord and manipulate public opinion. Finally, the cyber dimension needs to be addressed, as it is a critical component of a country's resilience and ability to counter hybrid threats. Whether – and if so, how – a country's technological infrastructure and connectivity influence its vulnerability to cyber-based interference needs to be assessed.

After identifying and analysing threats and vulnerabilities, **defence mechanisms** are considered. **The first step is to identify the existing strategies, policies, and institutions in place to defend a country against foreign interference. The second step is to analyse the effectiveness of these mechanisms in detecting, preventing, and mitigating interference attempts.** When conducting an analysis of defence mechanisms, it is important to analyse whether there are any gaps or weaknesses in the country's defence mechanisms and, if so, what they are. In this context, it is worth analysing how resilience is promoted in the population, including such dimensions as media literacy and critical thinking.

Address

Coordination and cooperation comprise an important dimension for successful countering of complex problems such as hybrid threats and foreign influence and interference. Identifying and analysing structures and practices are complex tasks, not least because they tend to be unique depending on each country's context. However, areas that need to be addressed include how relevant government agencies, intelligence services, and law enforcement bodies are coordinated and whether joint national capabilities have been developed across the hybrid threat spectrum to identify, analyse, and counter such activities. For example, is information sharing coordinated, and is there cooperation and coordination between the response capability of government leadership, intelligence, cyber defence, counter-influence agencies, and other key societal actors? At the societal level, the role of civil society organisations, media outlets, and other non-state actors in supporting defence against foreign interference must be considered.

It is also important to acknowledge that coordination and cooperation are not only national affairs but also international ties with countries and organisations. Thus, it needs to be explored whether there are collaborations and mechanisms in place for sharing intelligence, information, and best practices with international partners and allies and, if so, to what extent they are effective.

Legal and policy framework is a crucial part of the analysis, creating the frame for resilience and countering of hybrid threats and foreign interference. It is important to map and understand the kind of legal frameworks and regulations in place to counter foreign interference and protect national security. What are these legal and policy frameworks, and how well do existing laws and policies address the evolving nature of foreign interference? This aspect includes technological

dimensions, addressing whether they are able to account for emerging technologies used by adversaries.

Evaluate

Finally, **impact and effectiveness need to be evaluated, being the goal of the other five dimensions.** Here, we first need to analyse the impact of foreign interference on the country's political stability, public opinion, and democratic processes. Then, the focus shifts to how the country has responded to specific instances of foreign interference and what lessons have been learned. Have existing defence mechanisms effectively countered foreign interference? Finally, it needs to be asked how citizens perceive the effectiveness of defence measures and their confidence in the government's ability to protect against foreign interference.

The above analytical framework can be operationalised through a step-by-step method that converts concepts into actions. The next section lays out this method using a practical analytical guidebook.

ANALYTICAL GUIDEBOOK

While the preceding sections outline the conceptual logic of the AAE model, practitioners also require tools that support systematic and replicable analysis (Figure 6 below). The guidebook operationalises the framework, translating each phase into a structured set of guiding questions designed to support comprehensive assessments and inform decision-making in practice.

Figure 6: Analytical guidebook for countering foreign interference

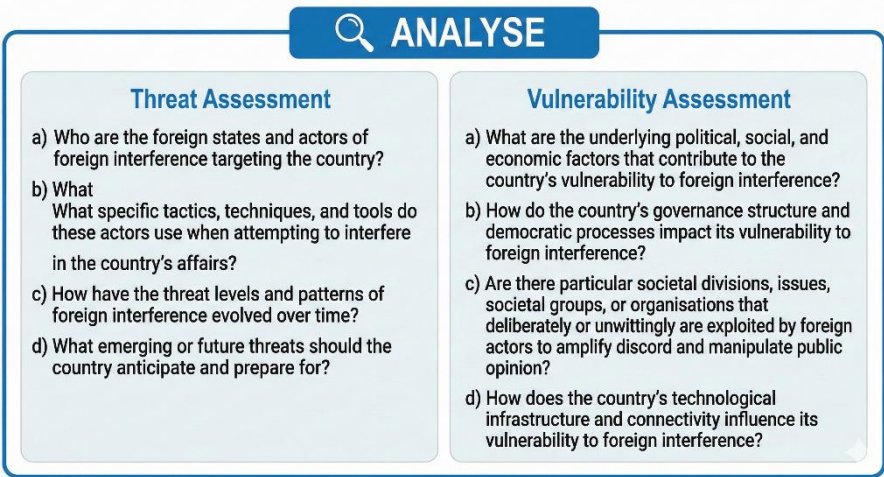


Source: Authors' model, developed from Palmertz et al. (2024). Image created in Gemini.

In the following pages, you find the overarching guidebook followed by a breakdown of the respective analysis, address and evaluate steps one by one (Figure 7-8. Also see Appendix 1).

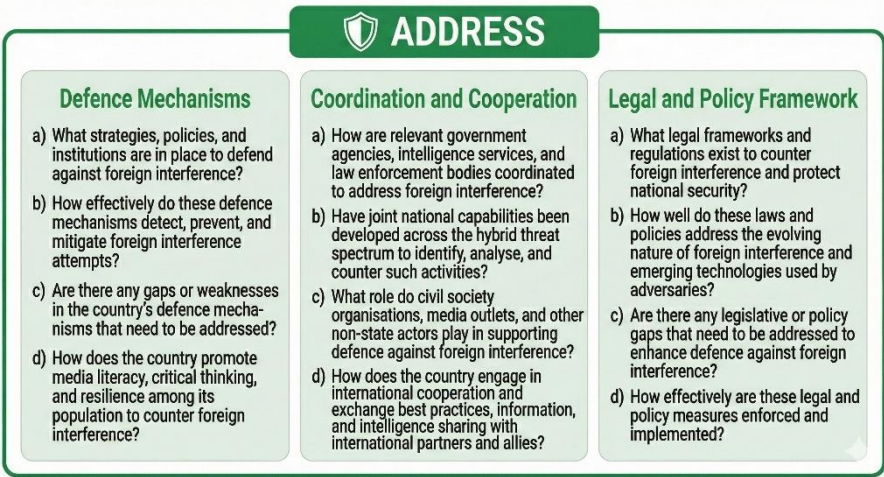
In addition to the above guidebook, an analytical template is also available, which addresses each key question through a three-step approach: analysis, impact assessment, and proposed action. The aim is to ensure a holistic and logical progression – from understanding the problem, to assessing its significance, and finally proposing actionable solutions. The analytical template is available in the authors' report *Building Resilience and Psychological Defence: An Analytical Framework for Countering Hybrid Threats and Foreign Influence and Interference*, available for free download at <https://fhs.diva-portal.org/smash/record.jsf?pid=diva2%3A1846756>.

Figure 7: Analytical guidebook - Analyse



Source: Authors' model, developed from Palmertz et al. (2024). Image created in Gemini.

Figure 8: Analytical guidebook - Address



Source: Authors' model, developed from Palmertz et al. (2024). Image created in Gemini.

Figure 9: Analytical guidebook - Evaluate

The graphic features a purple header bar with a clipboard icon and the word 'EVALUATE' in white. Below this is a light purple rounded rectangle containing the title 'Impact and Effectiveness' and a list of four evaluation questions.

EVALUATE

Impact and Effectiveness

- a) What are the measurable impacts on the country's political stability, public opinion, and democratic processes, taking into account the second-order and unintended effects of foreign interference?
- b) How has the country responded to specific instances of foreign interference, and what lessons have been learned?
- c) Have the defence mechanisms put in place shown demonstrable effectiveness in countering foreign interference?
- d) How do the country's citizens perceive the effectiveness of defence measures and their confidence in the government's abilities?

Source: Authors' model, developed from Palmertz et al. (2024). Image created in Gemini.

CONCLUSION

There is no definitive recipe for protecting against hybrid threats and cognitive warfare or for building psychological defence or resilience. Nor can a single actor or organisation succeed in this task alone. We must continuously adapt as adversaries, technologies, and threat patterns evolve, and as the interaction between attack and response shifts over time, as captured in the hybridity blizzard model.

How, then, do we handle these challenges in practice? The work must be pragmatic, flexible, and explicitly involve the whole of society, involving multiple actors beyond government agencies and intelligence and security services across sectors and levels, both nationally and internationally. Hybrid threats and cognitive warfare are designed to come as a surprise, and when countermeasures succeed, the adversary changes its pattern of attack. This, in turn, requires not only a strategy but also governance arrangements and routines that enable the system to learn, adjust, and re-prioritise as attacks and vulnerabilities shift over both the short and long terms – the very dynamics which the hybridity blizzard model seeks to capture. The most likely path to success can be found in focusing on building whole-of-society defence capabilities: the greater a society's psychological defence, resilience, and capacity for recovery, the greater and more sustainable the effect of countermeasures.

It is also crucial that governments and government agencies, including intelligence and security services, cooperate with key international and regional partners, both within and beyond their areas of operation. Cooperation across sectors and levels is necessary, and barriers created by traditional boundaries must be reduced. This includes reducing the legal, bureaucratic, and classification barriers that unnecessarily inhibit timely information sharing and coordinated responses. Weaknesses in defence against future hybrid threats and cognitive warfare are most often found in the seams between sectors and levels, and attacks against these can be directed to maximise the chance of success. Closing these seams, through shared situational awareness, joint training, and routinised cross-sector interaction, must be understood as a core task of national preparedness. The solution is cooperation between and within the military, political, and economic spheres; civil society; and actors in the information domain—across both the

public and private sectors, and between local and regional levels, all the way up to the national and international levels.

This report aimed to support such solutions by (1) introducing a six-dimensional AAE framework for understanding foreign interference and hybrid threats, (2) operationalising it into a modular analytical guidebook, (3) translating it into a concise analytical template for practitioners, and (4) situating these tools in relation to the hybridity blizzard model, which conceptualises the evolving interaction between antagonistic hybrid activity, vulnerabilities, and defensive responses.

Taken together, the framework, guidebook, template, and hybridity blizzard model offer a common language and practical structure for comparing cases, identifying gaps, and linking analysis to action across the public–private spectrum. They are not intended as a final blueprint but as a shared starting point that can and should be adapted to different national contexts and updated as threat actors, technologies, and practices evolve.

Taken together, the tools outlined in this report are designed to provide a concrete basis for moving from early warning to absorption and resilience across the public–private spectrum. To convert insights into capabilities, three near-term implementable steps are suggested.

(1) Institutionalise the hourglass workflow – linking intelligence analysis, tailored dissemination, and reception/absorption among key societal actors – as the default interface between analysis → tailored dissemination → reception/absorption across priority sectors.

(2) apply the three-step analytical template (Analysis → Impact Assessment → Proposed Action) to all priority questions and track a small, shared set of indicators for psychological defence and resilience.

(3) Run regular ‘blizzard’ drills – exercises built around ambiguous, multi-vector scenarios that mirror the turbulent interaction described in the hybridity blizzard model – which stress ambiguous, multi-vector scenarios and test hand-offs across local–national–international levels. These steps link this conclusion directly to the practical analytical guidebook presented above and the authors’ template, enabling practitioners to move from warning to coordinated action with measurable effects.

REFERENCE LIST

Backes, O. and Swab, A. (2019) *Cognitive Warfare: The Russian Threat to Election Integrity in the Baltic States*. Cambridge, MA. Available at: https://www.belfercenter.org/sites/default/files/pantheon_files/2019-11/CognitiveWarfare.pdf (Accessed: 9 September 2025).

Claverie, B., Prébot, B., Buchler, N., and Du Cluzel, F. (eds.) (2021) *Cognitive Warfare: The Future of Cognitive Dominance*. First NATO scientific meeting on Cognitive Warfare (France), 21 June.

Claverie, B. and Du Cluzel, F. (2021) ‘“Cognitive Warfare”: The Advent of the Concept of “Cognitics” in the Field of Warfare’, in B. Claverie, B. Prébot, N. Buchler, and F. Du Cluzel (eds.) *Cognitive Warfare: The Future of Cognitive Dominance*. First NATO scientific meeting on Cognitive Warfare (France), 21 June, 2:1-2:8.

Hoffman, F. (2025) ‘Assessing “Cognitive Warfare”’, *Small Wars Journal*, 14 November. Available at: <https://smallwarsjournal.com/2025/11/14/assessing-cognitive-warfare/> (Accessed: 22 November 2025).

Ivan, C., Chiru, I., and Arcos, R. (2021) ‘A Whole of Society Intelligence Approach: Critical Reassessment of the Tools and Means Used to Counter Information Warfare in the Digital Age’, *Intelligence and National Security*, 36(4), pp. 495–511. doi: 10.1080/02684527.2021.1893072.

Nilsson, N. (2025) *Intelligence and Strategic Communication*. NATO Strategic Communications Centre of Excellence, Riga.

Nilsson, N., Weissmann, M., and Palmertz, B. (2026) ‘Hybrid Threats and the Intelligence Community: Priming for a Volatile Age’, *International Journal of Intelligence and CounterIntelligence*, 39(1), pp. 109-131. doi: 10.1080/08850607.2024.2435265.

Palmertz, B., Weissmann, M., Nilsson, N., and Engvall, J. (2024) *Building Resilience and Psychological Defence: An Analytical Framework for Countering Hybrid Threats and Foreign Influence and Interference*. Lund University Psychological Defence Research Institute, Lund. Available at: <https://fhs.diva-portal.org/smash/record.jsf?pid=diva2%3A1846756> (Accessed: 29 November 2025).

Weissmann, M. (2025) 'Future Threat Landscapes: The Impact on Intelligence and Security Services', *Security and Defence Quarterly*. 49(1), pp. 40–57. doi: 10.35467/sdq/197248.

Weissmann, M. (2024) 'Framtida hotbilders påverkan för säkerhetstjänsterna', in H. Häggström (ed.) *Framtidens säkerhetstjänst i totalförsvaret*. Swedish Defence University Report Series, Stockholm, pp. 38–67. Available at: <https://fhs.diva-portal.org/smash/get/diva2:1846156/FULLTEXT01.pdf> (Accessed: 29 November 2025).

Weissmann, M., Nilsson, N., and Palmertz, B. (2021) 'Moving out of the Blizzard: Towards a Comprehensive Approach to Hybrid Threats and Hybrid Warfare', in M. Weissmann, N. Nilsson, B. Palmertz, and P. Thunholm. (eds.) *Hybrid Warfare: Security and Asymmetric Conflict in International Relations*. I.B. Tauris, London.

APPENDIX 1: ANALYTICAL GUIDEBOOK

ANALYSE

Threat Assessment

- ▷ a) Who are the foreign states and actors of foreign interference targeting the country?
- ▷ b) What specific tactics, techniques, and tools do these actors use when attempting to interfere in the country's affairs?
- ▷ c) How have threat levels and patterns of foreign interference evolved over time?
- ▷ d) What emerging or future threats should the country anticipate and prepare for?

Vulnerability Assessment

- ▷ a) What underlying political, social, and economic factors contribute to the country's vulnerability to foreign interference?
- ▷ b) How do the country's governance structure and democratic processes impact its vulnerability to foreign interference?
- ▷ c) Are particular societal divisions, issues, societal groups, or organisations deliberately or unwittingly manipulated by foreign actors to amplify discord and manipulate public opinion?
- ▷ d) How do the country's technological infrastructure and connectivity influence its vulnerability to foreign interference?

ADDRESS

Defence Mechanisms

- ▷ a) What strategies, policies, and institutions are in place to defend against foreign interference?
- ▷ b) How effectively do these defence mechanisms detect, prevent, and mitigate foreign interference?
- ▷ c) Do any gaps or weaknesses in the country's defence mechanisms need to be addressed?
- ▷ d) How does a country promote media literacy, critical thinking, and resilience among its population to counter foreign interference?

Coordination and Cooperation

- ▷ a) How are relevant government agencies, intelligence services, and law enforcement bodies coordinated to address foreign interference?
- ▷ b) Have joint national capabilities been developed across the hybrid threat spectrum, in areas such as:
 - Information sharing and fusion capabilities
 - Government leadership, intelligence, cyber defence, and counter-intelligence agencies, or other key societal actors).
- ▷ c) What role do civil society organisations, media outlets, and other non-state actors play in supporting defence against foreign interference?
- ▷ d) How does the country engage in international cooperation and intelligence processes, such as NATO, and intelligence with international partners and allies?

Legal and Policy Framework

- ▷ a) What legal frameworks and regulations exist to counter foreign interference and protect national security?
- ▷ b) How well do these laws and policies address the evolving nature of foreign interference and emerging technologies used by adversaries?
- ▷ c) Do any legislative or policy gaps need to be addressed to enhance defence against foreign interference?
- ▷ d) How effectively are these legal and policy measures enforced and implemented?

EVALUATE

Impact and Effectiveness

- ▷ a) What are the measurable effects on a country's political stability, public opinion, and democratic processes, taking into account the second-order and unintended effects of foreign interference?
- ▷ b) What innoate comments?
- ▷ a) What are the measurable effects on a country's political stability, public opinion, and democratic processes, taking into account the second-order and unintended effects of foreign interference?
- ▷ b) How has the country responded to specific instances of foreign interference and what lessons have been learned?
- ▷ c) Have the defence mechanisms in place shown demonstrable effectiveness in countering foreign interference?
- ▷ d) How do citizens perceive the effectiveness of defence measures and their confidence in the government's abilities?

ANALYSE



Threat Assessment

- a) Who are the foreign states and actors of foreign interference targeting the country?
- b) What
What specific tactics, techniques, and tools do these actors use when attempting to interfere in the country's affairs?
- c) How have the threat levels and patterns of foreign interference evolved over time?
- d) What emerging or future threats should the country anticipate and prepare for?

Vulnerability Assessment

- a) What are the underlying political, social, and economic factors that contribute to the country's vulnerability to foreign interference?
- b) How do the country's governance structure and democratic processes impact its vulnerability to foreign interference?
- c) Are there particular societal divisions, issues, societal groups, or organisations that deliberately or unwittingly are exploited by foreign actors to amplify discord and manipulate public opinion?
- d) How does the country's technological infrastructure and connectivity influence its vulnerability to foreign interference?



ADDRESS

Defence Mechanisms

- a) What strategies, policies, and institutions are in place to defend against foreign interference?
- b) How effectively do these defence mechanisms detect, prevent, and mitigate foreign interference attempts?
- c) Are there any gaps or weaknesses in the country's defence mechanisms that need to be addressed?
- d) How does the country promote media literacy, critical thinking, and resilience among its population to counter foreign interference?

Coordination and Cooperation

- a) How are relevant government agencies, intelligence services, and law enforcement bodies coordinated to address foreign interference?
- b) Have joint national capabilities been developed across the hybrid threat spectrum to identify, analyse, and counter such activities?
- c) What role do civil society organisations, media outlets, and other non-state actors play in supporting defence against foreign interference?
- d) How does the country engage in international cooperation and exchange best practices, information, and intelligence sharing with international partners and allies?

Legal and Policy Framework


- a) What legal frameworks and regulations exist to counter foreign interference and protect national security?
- b) How well do these laws and policies address the evolving nature of foreign interference and emerging technologies used by adversaries?
- c) Are there any legislative or policy gaps that need to be addressed to enhance defence against foreign interference?
- d) How effectively are these legal and policy measures enforced and implemented?

EVALUATE



Impact and Effectiveness

- a) What are the measurable impacts on the country's political stability, public opinion, and democratic processes, taking into account the second-order and unintended effects of foreign interference?
- b) How has the country responded to specific instances of foreign interference, and what lessons have been learned?
- c) Have the defence mechanisms put in place shown demonstrable effectiveness in countering foreign interference?
- d) How do the country's citizens perceive the effectiveness of defence measures and their confidence in the government's abilities?



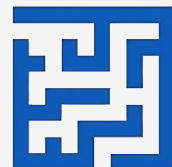
This report consolidates key takeaways from five publications authored by members of the Hybrid Threats Research Group into a single practitioner's toolbox for countering hybrid threats and cognitive warfare and for strengthening psychological defence and resilience. The toolbox brings together models developed and published by the group into a single, practitioner-focused guide for countering hybrid threats, cognitive warfare, and foreign interference. It presents the group's core analytical models in a clear, ready-to-use format.

Hybrid Threats Research Group
Stockholm
www.hybridthreatsresearch.com

ISBN 978-91-531-7376-2 (print)
ISBN 978-91-531-7377-9 (electronic)



9 789153 173762



**HYBRID
THREATS
RESEARCH
GROUP**