

Defending Europe Against Hybrid Warfare

October 2026



Hybrid CoE

The European Centre of Excellence
for Countering Hybrid Threats

This publication is a Science for Policy report by the Joint Research Centre (JRC), the European Commission's science and knowledge service, prepared together with the European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE). It aims to provide evidence-based scientific support to the European policymaking process.

The scientific output expressed does not imply a policy position of the European Commission nor Hybrid CoE. Neither the European Commission nor any person acting on behalf of the Commission or Hybrid CoE is responsible for the use that might be made of this publication. For information on the methodology and quality underlying the data used in this publication for which the source is neither Eurostat nor other Commission services, users should contact the referenced source. The designations employed and the presentation of material do not imply the expression of any opinion whatsoever on the part of the European Union or the Member States.

CONTACT INFORMATION

European Commission, Joint Research Centre (JRC)

<https://joint-research-centre.ec.europa.eu>

Directorate E – Societal Resilience and Security

JRC.E.7 – Defence and External Security

Contact: Julien Theron

E-mail: JRC-E7-SECRETARIAT@EC.EUROPA.EU

Joint Research Centre

<https://joint-research-centre.ec.europa.eu>

JRC148340

EUR 40871

Print ISBN 978-92-68-44034-6 ISSN 1018-5593 doi:10.2760/0739664 KJ-01-26-414-EN-C

PDF ISBN 978-92-68-43902-9 ISSN 1831-9424 doi:10.2760/3158614 KJ-01-26-414-EN-N

Luxembourg: Publications Office of the European Union, 2026

© European Union, 2026



The reuse policy of the European Commission documents is implemented by the Commission Decision 2011/833/EU of 12 December 2011 on the reuse of Commission documents (OJ L 330, 14.12.2011, p. 39). Unless otherwise noted, the reuse of this document is authorised under the Creative Commons Attribution 4.0 International (CC BY 4.0) licence (<https://creativecommons.org/licenses/by/4.0/>). This means that reuse is allowed provided appropriate credit is given and any changes are indicated.

All figures are made by the authors (JRC).

How to cite this report: Theron, J., Aho, A., Savolainen, J., Petit, F., De Angelis, A. et al., *Defending Europe Against Hybrid Warfare*, Publications Office of the European Union, Luxembourg, 2026, <https://data.europa.eu/doi/10.2760/3158614>, JRC148340.

Defending Europe Against Hybrid Warfare

Authors

Julien Théron (European Commission Joint Research Centre)
Aleksi Aho (European Centre of Excellence for Countering Hybrid Threats)
Jukka Savolainen (European Centre of Excellence for Countering Hybrid Threats)
Frédéric Petit (European Commission Joint Research Centre)
Alessandra De Angelis (European Commission Joint Research Centre)
Georgios Valsamos (European Commission Joint Research Centre)

Contributors

Rainer Jungwirth (European Commission Joint Research Centre)
Stefano Ruberto (European Commission Joint Research Centre)

Reviewers

Teija Tiilikainen (European Centre of Excellence for Countering Hybrid Threats)
Georgios Giannopoulos (European Commission Joint Research Centre)
Mikko Tyrväinen (European Centre of Excellence for Countering Hybrid Threats)
Ana Lisa Vetere Arellano (European Commission Joint Research Centre)

CONTENTS

- ABSTRACT.....4
- FOREWORD.....5
- EXECUTIVE SUMMARY.....6
- INTRODUCTION.....10
 - A rapidly changing and challenging international security environment.....10
 - At the operational level: saturation, high-impact operations and cascading effects.....11
 - Saturation: the volume variable.....11
 - Cascading effects: the time variable.....12
 - High impact operations: the intensity variable.....14
 - At the strategic level: the rise in intensity to hybrid warfare.....14
- 1. PROACTIVE ANTICIPATION.....18
 - 1.1. Operationalising resilience.....19
 - 1.2. Introducing deterrence.....20
 - 1.2.1. Why deterrence is essential to counter hybrid threat operations.....22
 - 1.2.2. Primary concepts of deterrence.....23
 - 1.2.3. Secondary concepts of deterrence.....24
 - 1.2.4. Operationalising deterrence.....27
 - 1.3. Articulating resilience and deterrence.....30
 - 1.3.1. Combining resilience and deterrence.....31
 - 1.3.2. Proactive anticipation in practice.....36
- 2. ACTIVE DEFENCE.....39
 - 2.1. Detection.....39
 - 2.2. Identification.....40
 - 2.3. Determination.....41
 - 2.4. Recovery.....41
 - 2.5. Attribution.....41
- 3. REACTIVE RESPONSE.....46
- 4. RESILIENCE-DETERRENCE STRATEGY.....48
 - 4.1. Shifting the adversary's calculus.....48

4.2. The strategy.....	49
4.3. Risks.....	49
5. CASE STUDIES.....	50
5.1. Case study 1: resilience only.....	50
5.2. Case study 2: deterrence by denial.....	51
5.3. Case study 3: early detection and deterrence by disclosure against a high impact operation.....	52
5.4. Case study 4: deterrence by punishment against a high impact operation.....	53
6. CONCLUSIONS.....	54
REFERENCES.....	55
LIST OF ABBREVIATIONS.....	67
LIST OF FIGURES.....	68
LIST OF TABLES.....	69
ANNEXES 1: MEASURES FOR RESILIENCE.....	70
Resilience in the civic space.....	70
Education.....	70
Information.....	71
Participation.....	71
Resilience in the governance space.....	72
Whole of government.....	72
Social contract.....	72
Preparedness and response.....	72
Trust building.....	73
Resilience in the services space.....	73
Investments.....	73
Public-private partnerships.....	74
Supply of goods.....	74
Access to essential services.....	74
ANNEX 2: COUNTERMEASURES FOR DETERRENCE.....	75



“As hybrid attacks are escalating, Europe is taking action to protect itself. Our Emergency Security Protocol creates a solidarity mechanism against hybrid warfare. So we can respond to threats to our national security firmly and with one voice. Because in unity lies our strength.”

Ursula von der Leyen

President of the European Commission



ABSTRACT

In an increasingly complex and challenging security environment, the escalation of hybrid threats into hybrid warfare poses a growing risk to European democracies. In this context, reliance solely on resilience is insufficient, and an effective deterrence scheme is necessary.

This report undertakes an in-depth examination of the European security environment's structural transformation, revealing novel requirements for enhanced resilience and presenting conceptual opportunities for deterrence against hybrid threats.

Furthermore, it presents a resilience-deterrence strategy (RD strategy) that combines proactive, active and reactive steps. While this study primarily focuses on the strategic level, it also proposes operational measures for resilience and countermeasures for deterrence, thereby offering a holistic framework for implementation.

FOREWORD



Andrius Kubilius

European Commissioner for Defence and Space

Europe faces a sustained campaign of Russian sabotage, cyberattacks and interference. Recent attacks involving explosives and arson show how directly this campaign threatens our security. Russia seeks to disrupt the production and delivery of weapons to Ukraine, including through physical attacks in Europe. Moscow has openly threatened European arms factories supplying Ukraine. The danger is especially visible on our eastern flank, but it concerns the whole of Europe.

Protecting this infrastructure is part of our defence readiness. Our ability to defend ourselves and support Ukraine depends on factories that can produce, energy networks that can supply them, and transport routes that remain open. Ukraine's experience shows why keeping these systems functioning under attack is essential.

Resilience helps us withstand disruption and recover. Deterrence changes the aggressor's calculation. That is why we must move from resilience to deterrence. We need to make attacks harder to carry out, identify and expose those responsible, and impose costs through lawful and proportionate responses. Collective defence can also apply to sufficiently serious hybrid attacks. Yet many hostile operations are designed to exploit uncertainty over responsibility and severity, and to delay or even undermine collective self-defence.

Repeated attacks cannot become an accepted part of Europe's security environment. We must recognise the cumulative effects of hostile activities across borders and respond to the campaign they form. We need clearer procedures to assess threats jointly, coordinate protective action and agree lawful consequences, including when collective defence has not been invoked. Uncertainty over attribution must not prevent immediate protective action.

A great step in this direction is the new science-for-policy report by the European Commission's Joint Research Centre (JRC) and the European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE). A third in a series of conceptual flagship reports, the report contains actionable analyses for a deeper understanding of the current situation and trends.

The report proposes to policy- and decision-makers a scientifically robust resilience-deterrence strategy, which could contribute to the European Union's deterrence and defence against hybrid threat operations by both state and non-state actors. By incorporating deterrence into our overall strategy, we can effectively contain hybrid warfare and protect our interests, as well as those of our allies, in Europe and worldwide.

I thank the teams at the JRC and Hybrid CoE for their outstanding work on this report. Their work can help Europe strengthen its ability to act together, protect its defence readiness and maintain its support for Ukraine.

EXECUTIVE SUMMARY

A rapidly evolving and challenging international security environment

The rise of hybrid threats signals a new era in European security. Although hybrid threat operations remain below the threshold of formally declared war, they represent a fundamental change in the security environment.

The international security environment, having shifted from cooperation to competition, now exhibits signs of escalating towards confrontation. This deteriorating international security environment can be characterised by a challenging and rapidly evolving context, the complexity of adversarial strategies, as well as escalated hybrid threats operations.

At the operational level: Saturation, high impact and cascading effects

Three trends characterise the current evolution of hybrid threats at the operational level: saturation, cascading effects and high-impact operations.

Saturation: the volume variable

Saturation can be understood as the result of large-volume operations, possibly conducted by several actors, in coordination or not, designed to overload the target's defences and exhaust its resources.

Actors may also target a group of democracies by attacking their cooperation links, thereby disrupting collective security's alliances or organisations. The aim of saturation is to exhaust democracies and wear down their capacity to endure attacks, absorb their impact, recover and adapt.

Cascading effects: the time variable

Cascading effects can be understood as the diverse negative fallouts from a hybrid threat operation, beyond its original objective, which can be weaponised further by the same or other actors to conduct new operations, including in other domains, regardless of the original operation's effectiveness.

They can be designed by the attacker and weaponised to serve the initial objective or identified opportunistically after observing the impact of initial attacks and exploited in other domains.

High impact operations: the intensity variable

High impact operations (HIO) are hybrid threat operations intended to inflict significant harm on democratic societies, challenging resilience and producing lasting cascading effects. Denied or not by the attacker, depending on its intention to deceive the defender or subjugate it cognitively, HIOs aim at shocking societies and decision-makers and paralysing their capacity to defend and respond.

They exploit the linearity of escalation theory, using deception and surprise to create key disruptions. While signals still exist, HIOs demand a reinforced cognitive ability to anticipate and analyse attacks properly. They might be kinetic attacks as well as attacks of an immaterial nature. Designed to leave a profound, lasting impact on democratic societies.

At the strategic level: rise of intensity to hybrid warfare

At the strategic level, several studies conducted since 2022 show that hybrid attacks against EU MS have intensified. Analysts and scholars identify

two parallel trends: one domain dependent and one tool dependent. On the policy side, the concept of hybrid warfare has been endorsed. EU MS government and state officials use the concepts of ‘hybrid warfare’ or ‘hybrid war’ to qualify the situation.

The Hybrid CoE defines hybrid warfare as “a subset of hostile activities against a state, falling under the category of hybrid threats but representing an escalated phase. These activities may also involve military means and the use of chemical, biological, radiological, and nuclear (CBRN) threats, marking a shift from under-detected or unattributed activities to overt coercion. Hybrid warfare represents the “hard end” of the escalation spectrum of hybrid threat activity” (*)

The resilience-deterrence (RD) strategy

Countering hybrid warfare has therefore become an existential struggle for European democracies. It now necessitates a paradigm shift, from merely adapting to past attacks to deterring and preparing for future ones, which will be even more challenging. In this respect, the RD strategy is intended to operate as a self-reinforcing loop, with several returns that consolidate resilience and deterrence at every one of its three steps.

1. Proactive anticipation, combining in advance resilience and deterrence.
2. Active defence, optimising the immediate handling of hybrid threat operations.
3. Reactive response, imposing cost to the adversary to prevent future attacks to occur again.

1. Proactive anticipation

Proactive anticipation seeks to dissuade future hybrid threat operations while still preparing for the possibility that they may occur. In this step, resilience and deterrence converge, because resilience creates the denial capability that underpins deterrence.

Indeed, without deterrence, resilience would have

to absorb the ever-increasing consequences of hybrid threat operations. Without resilience, deterrence could aim to prevent attacks and their effects, but, if it fails, societies are left vulnerable.

Deterrence and resilience constitute a single system as they inevitably influence each other. Enhancing resilience automatically strengthens deterrence, while a higher level of deterrence enables more robust resilience.

Deterrence and resilience must be closely coordinated from a very early stage at the strategic level. The success of a tailored security strategy depends on this upstream strategic coordination.

Ten operational requirements can improve proactive anticipation.

- Strategic depth
- Integration of disruption
- Complexity management
- Questioning of certainties
- Implementation of anticipation
- Adaptation celerity
- Political resolve
- Strategic decisiveness
- Whole-of-society approach
- Norms and entanglement

The concept of deterrence induces multiple possible approaches that can be tailored depending on the strategic and operational situation.

Primary concepts of deterrence

- Deterrence by denial. Preventing the performance of a successful attack.
- Deterrence by punishment. Imposing sufficient costs to prevent future attacks.

(*) Hybrid CoE (n.d.), ‘Hybrid warfare’, The European Centre of Excellence for Countering Hybrid Treats (Hybrid CoE), no date. www.hybridcoe.fi/hybrid-warfare/

Secondary concepts of deterrence

- **Absolute deterrence.** Averting an attack by building capabilities in anticipation.
- **Restrictive deterrence.** Constraining the intensity of an attack to make it tolerable.
- **Cumulative deterrence.** Concentrating deterring efforts to limit the threshold of harm.
- **Deterrence by disclosure.** Exposing incoming attacks to sap the adversary's denial.
- **Deterrence by stratcom.** Signalling resolve and readiness to counter an attack.
- **Integrated deterrence.** Displaying powerful deterring strength.
- **Internalised deterrence.** Quietly setting up internal preparedness.
- **Extended deterrence.** Strengthening collective security to dissuade the attacker.
- **Deterrence by inducement.** Incentivising the adversary to target the most resilient area.

2. Active defence

An active defence should be carried out during an attack and immediately afterwards, as swiftly and fluidly as possible. It is organised around three stages (detection–identification–determination (DID)) and two additional elements with specific roles (recovery and attribution).

- **Detection.** Indicators capture signals that an event is occurring.
- **Identification.** Operational-level analysts study the event, its context and its precedents to understand which actor or group of actors is behind it, recognising that it is a hostile operation.
- **Determination.** Strategic-level senior analysts consider the event alongside other ongoing or recent hostile operations using different tools in different domains, highlighting the hybridity of the operation.

The two additional elements are essential and have specific characteristics.

- **Recovery.** Initiated at the detection stage and potentially lasting for a long period, the recovery first ensures business continuity and then restores full capacity. Even seemingly innocuous actions can be harmful, as they may erode public trust over the long term or provide opportunities for the cascading effects. Recovery is therefore an essential task and should be pursued as much as possible.
- **Attribution.** Following the determination stage, attribution is the political statement by decision-makers that officially assigns responsibility to the actor or group of actors behind the hybrid threat operation. Hybrid threat operations gain their greatest strength from deniability. By obscuring the true source of an operation, the aggressor can keep the target in a sub-threshold environment and pretend to perceive any response as unjustified and escalatory. This progressive strategic erosion of the target proceeds until the attacker's objectives are achieved. Citizens suffer the consequences of hybrid threat operations without knowing who is responsible for them. Yet attribution is essential for deterrence, as it is generally difficult to respond to hybrid threat operations without attribution, and attribution also underpins resilience. Attribution legitimises policy choices

Although these five elements do not prescribe a rigid procedure – each European security actor at every level follows its own processes – they outline the essential stages required to actively defend against hybrid threat operations.

3. Reactive response

To prevent an escalation in intensity and to avoid a slide into more severe conflicts, a response strategy should amplify the adversary's costs through deterrence. Europe must therefore act swiftly to increase cost imposition within the grey zone by deploying countermeasures. Reactive response follows the attack and constitutes a measured, proportionate response that must be more impactful than the original aggression in order to achieve a deterrent effect.

A non-exhaustive but comprehensive list of operational countermeasures is provided in the Annex 2 of the report. Rather than covering all measures, it outlines the instruments that could be used in a democratic framework and shows examples of what responses can be taken to hybrid threat operations. Below are some examples of the countermeasures for deterrence proposed by the report.

- **Regulating actions within the framework of common organisations** [long-term deterrent]. Beyond diplomatic efforts such as naming and shaming, the UN and regional organisations offer mechanisms for legal action that can establish and condemn violations of international law. This approach sends a clear message that unchecked behaviour will not be tolerated.
- **Military procurement and stockpiling initiatives** [proactive measure]. This measure enhances and sustains constantly developing procurement, the stockpiling of weaponry and ammunition, and medical countermeasures (including but not only CBRN) to ensure long-term combat readiness, thereby contributing to deterrence efforts.
- **Tripwire force deployment in Member States and partner countries** [strategic signal]. As already implemented, a limited tripwire force can have a deterrent effect by signalling to the adversary that any intervention might entail unwanted consequences. This approach can be applied across land, sea, air and space military domains.
- **Sanctions against institutions and companies involved in hybrid threat operations** [rapid activation]. Strategic institutions and sanctioned companies could be legally or technically blocked in response to hybrid threat operations.
- **Journalism media consortia** [long-term deterrent]. Collaborations between EU media outlets and exiled independent media can make it possible to conduct investigations, leveraging the sources of the latter and the distribution networks of the former.

Shifting the adversary's calculus

The aim of the Resilience-Deterrence Strategy is to shift the adversary's calculus by delivering multiple effects:

- **Reduced deniability** – As the likelihood of successful attribution increases, the adversary is likely to become more cautious about future hostile intentions.
- **Capability depreciation** – The combined pressure of resilience and deterrence compels the adversary to reassess its capabilities and the resources it allocates.
- **Internal institutional pressure** – Repeated failures generate pressure on the adversary's staff, prompting a shift towards softer targets, which should themselves be covered by collective security.
- **Ally coherence revelation** – An enhanced counter-strategy reshapes the adversary's perception of the coalition, underscoring a stronger resolve and a more robust commitment to democracy than was previously anticipated.
- **Compressed time horizon** – Long-term operations become less attractive when they are reduced to a negligible effect or incur prohibitive costs.

INTRODUCTION

The rise of hybrid threats signals a new era in European security. The four activities defined in the report *The Landscape of Hybrid Threats: A Conceptual Model* (Giannopoulos et al., 2023) – interference, influence, operations and war/warfare – are jointly employed by hostile actors against European democracies, whether they are EU Member States or partner countries. Although these activities remain below the threshold of formally declared war, they became overall critical. As a result, hybrid threat operations now pose an existential threat to European democracies.

By employing ‘the full spectrum of hybrid threats’ (Niinistö, 2024, p. 103), adversaries seek to induce governance paralysis, service failure and civic collapse. The aim is no longer to manipulate political decision-making in a favourable manner. Instead, the parallel offensive by state and non-state actors against European societies seeks to break their solidarity and dismantle them one by one. A new strategy countering hybrid threat operations is called for to ensure democratic security.

A rapidly changing and challenging international security environment

The international security environment, having shifted from cooperation to competition, now exhibits signs of escalating towards confrontation. This deteriorating international security environment can be characterised by several trends:

- **A challenging and rapidly changing context**
 1. the increasing fragility of democracies amidst a global trend of autocratisation (Nord et al., 2025),
 2. the alignment of autocratic state and non-state actors, despite their pursuit of differing or antagonistic political objectives (Theron, 2021),
 3. more assertive antagonistic rhetoric from adversaries, alongside a paradoxical continued denial of hybrid threat operations,
 4. the progressive disappearance of declared war in favour of conflict in the ‘grey zone’ (D’Cunha et al., 2025), leading to eroded international law regulatory mechanisms;
- **The complexity of adversarial strategies:**
 5. the application of external strategic pressure alongside efforts to foster internal polarisation,
 6. the covert infiltration of European societies by intelligence operatives and their local agents, which may include agents, ideologically aligned personalities, ‘useful idiots’ or individuals used as low-level operatives or ‘disposable agents’⁽¹⁾,
 7. systematic attacks on cooperation mechanisms, including the European Union (EU), the North Atlantic Treaty Organisation (NATO), and subregional and international platforms,
 8. specific strategies targeting European democracies that support partners such as Ukraine and Taiwan, linking hybrid threat operations to the development of extra-EU geopolitics;

⁽¹⁾ Permitting higher deniability and exploiting local discord for disinformation, these new local actors of hybrid attacks are ‘recruited on social media to target various countries with cyberattacks, arson, vandalism, sabotage and influence campaigns during elections’ (European Broadcasting Union 2025a).

• Escalated hybrid threat operations

9. operational inventiveness employing high-tech tools (e.g. cyberattacks, electronic warfare), mid-tech tools (e.g. drones) and low-tech tools (e.g. graffiti, balloons),
10. the synergistic effects of hybrid threat operations from diverse state and non-state actors,
11. a combination of kinetic and non-kinetic operations,
12. increasingly overt strategic intimidation in the military domain.

At the operational level: saturation, high-impact operations and cascading effects

Three trends characterise the current development of hybrid threats at the operational level: saturation effect, high-impact operations (HIOs) and cascading effects.

Saturation: the volume variable

A notable characteristic of the ‘rapidly deteriorating security environment’ (European Parliament, 2025a) is the ‘broader, coordinated, and long-standing hybrid campaigns aimed at threatening and undermining the security, resilience and democratic foundations of the EU, its Member States and its partners’ (Council of the European Union, 2025). The ‘worrying pattern of growing threats’ (European Commission, 2025a) was highlighted in the Strategic Compass (European External Action Service, 2022, p. 10).

Ultimately, the new threat landscape reveals attempts to saturate the European security ecosystem. Autocratic state and non-state actors adhere to the principle of *vincit qui patitur* (who perseveres, wins) – a principle that democracies often overlook despite Ukrainians demonstrating its relevance through their enduring fight (Cohen, 2024).

The concept of saturation is well documented in the information and cyber domains (Geers, 2011; Giles, 2016, p. 32). It also manifests in joint cyber-informational operations with a political dimension (Marzano, 2026).

Saturation has been observed in the legal (Sari, 2020), intelligence (Snyder, 2025), and economic domains (Jakóbowski et al., 2025) and raises a short-term concern for military defence (Bastita Cabanas et al., 2026), space (European Space Agency, 2026a, 2026b) and infrastructure (Euro-

pean Organisation for Security, 2024). Saturation has also already been framed as a comprehensive strategy (Muhić, 2025).

The aim of saturation is to exhaust democracies and wear down their capacity to endure attacks, absorb their impact, recover and adapt. In other words, resilience is massively targeted at the local, national and international levels to eventually overcome democratic societies’ resistance to autocracy.

Saturation can be understood as the result of large-volume operations, possibly conducted by several actors, in coordination or not, designed to overload the target’s defences and exhaust its resources. Actors may also target a group of democracies by attacking their cooperation links, thereby disrupting collective security’s alliances or organisations.

Figure 1 shows how, whether coordinated or not, autocratic state actors (regimes, pictured here as squares) and non-state actors (groups, pictured here as triangles) of different geopolitical weight collectively structure the threat landscape against Member States and their allies.

These attacks occur either through external means (e.g. through the cyber, information, diplomacy, military defence and/or legal domains) or internal destabilisation (e.g. the political, intelligence, social/societal and/or cultural domains).

Figure 1 depicts how multiple actors produce a kill web at the strategic level, saturating the defenders with attacks in order to divide and undermine them.

Cascading effects: the time variable

The new threat landscape is also characterised by the exploitation of cascading effects, which are particularly challenging to manage. By leveraging the interconnections between different domains, such exploitation amplifies the damage inflicted on democratic societies. As the report *Hybrid Threats: A Comprehensive Resilience Ecosystem* states, ‘hybrid threats aim to create cascading effects and exploit interconnections,’ necessitating that ‘a systemic approach is necessary’ to counter them (Jungwirth et al., 2023, p. 10).

Cascading effects can be designed by the attacker and weaponised to serve the initial objective (typ-

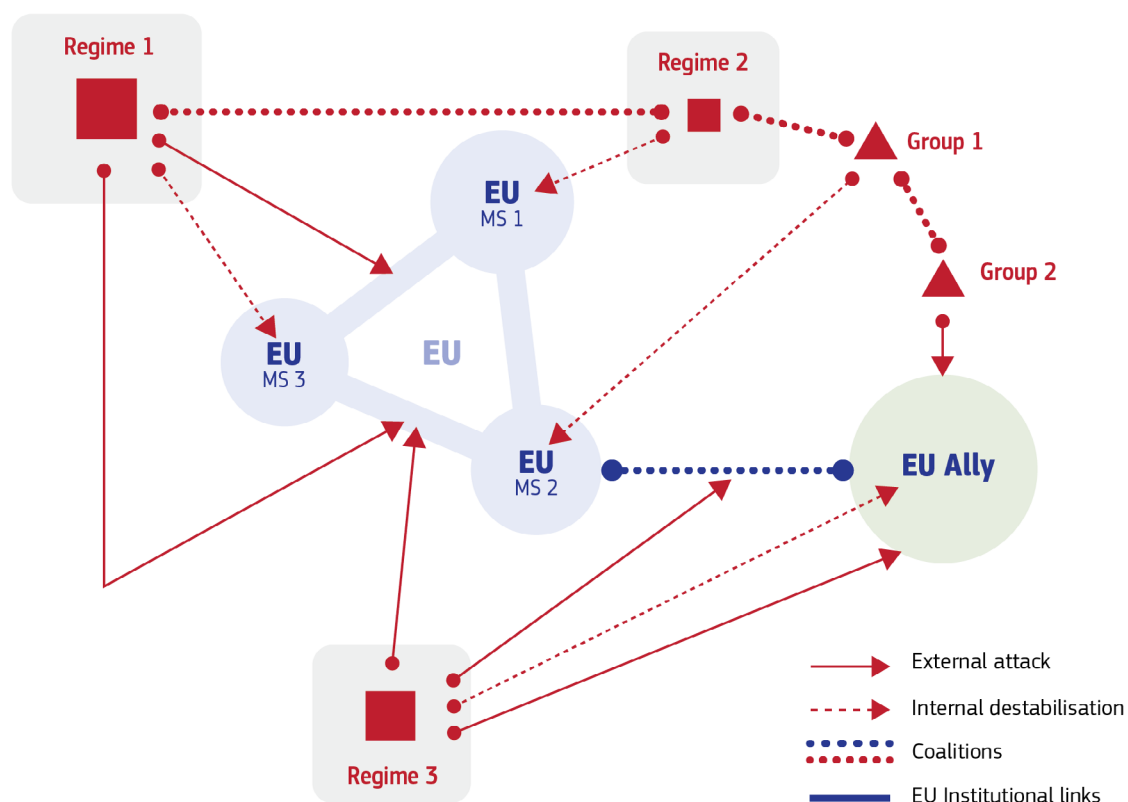
ically in the information and diplomatic domains) or identified opportunistically after observing the impact of initial attacks and exploited in other domains (e.g. social/societal or political domains).

Time is the key factor in exploiting past hybrid attacks with new ones, and the adversary's reactivity and adaptability are crucial for producing cascading effects. However, the longer the primary attack's impact, the easier it becomes to deploy secondary attacks.

Therefore, cascading effects are time-dependent and require prompt determination and highly reactive responses to break the chain.

Ignoring the cascading effects means letting a slow-building crisis erode the long-term ability to withstand and recover. Over time, the population becomes increasingly polarised, security and defence practitioners face mounting challenges, finances are diverted from normal governance, and

FIGURE 1
Multi-actor saturation of European security ecosystem (2)



Source: EU

(2) By attacking EU MS and their partners in multiple ways (e.g. internal destabilisation, external attacks against the country and/or against cooperation mechanisms), operations converge from diverse state and non-state actors.

decision-makers are exposed to an overwhelming combination of internal defiance and strategic intimidation.

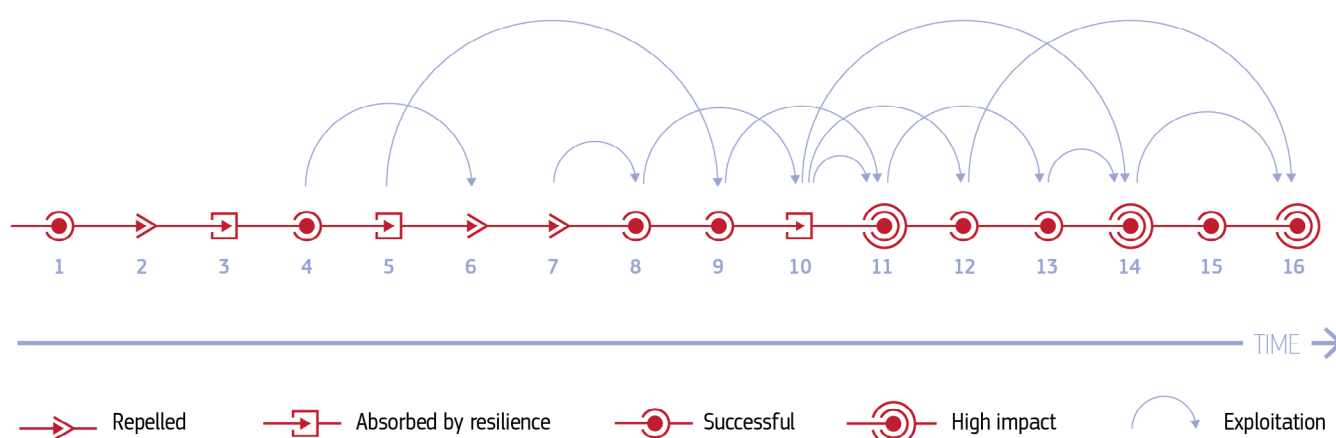
Cascading effects can be understood as the diverse negative fallouts from a hybrid threat operation, beyond its original objective, which can be weaponised further by the same or other actors to conduct new operations, including in other domains, regardless of the original operation's effectiveness.

Figure 2 shows how cascading effects can operate, weaponised from one to another or over the long term. These effects can capitalise on not only successful attacks but also repelled attacks or those absorbed with efficient resilience. If HIOs can be conducted independently of previous attacks, the adversary can also capitalise on multiple cascading effects to organise more HIOs. Ultimately, the multiplication of cascading effects over time overwhelms the defender, until it is in an inextricable situation where resilience is insufficient to prevent societal collapse.

Cascading effects can be exploited over the long term by diverse state and non-state actors, who may or may not have been involved in previous attacks. Indeed, 'the highly efficient systems of modern society are significantly interdependent' (Savolainen, 2025, p. 209), necessitating a comprehensive analysis of the threat landscape. Furthermore, this interdependency is evident not only within a society also but also between democratic partners, which are themselves highly interconnected.

The new threat landscape, therefore, reveals a systemic risk from interconnected hybrid threat operations constituting a network of threats (Theron, 2021) that can deeply undermine the stability of democratic societies.

FIGURE 2
Multiple exploitation of cascading effects



Source: EU

High impact operations: the intensity variable

More overtly aggressive actions can be called HIOs. Denied or not by the attacker, depending on its intention to deceive the defender or subjugate it cognitively, HIOs aim at shocking societies and decision-makers and paralysing their capacity to defend and respond. They exploit the linearity of escalation theory, using deception and surprise to create key disruptions. While signals still exist, HIOs demand a reinforced cognitive ability to anticipate and analyse attacks properly.

They might be kinetic attacks as well as attacks of an immaterial nature. Designed to leave a profound, lasting impact on democratic societies, HIOs challenge existing legal frameworks and requires robust anticipatory capabilities to reinforce deterrence and resilience.

The infrastructure that supports modern society is an attractive target for potential HIOs. Infrastructure collapse could occur because non-systemic failures might have cascading effects that result in longer recovery times. For example, in the event of power grid failure, systemic failure results from a coordinated, gradual build-up.

If communication lines are also dysfunctional, coordination is more difficult. After some time has elapsed, other systems would start losing their back-up power reserves and cease functioning. Such wider disturbances can be pre-planned and executed through coordinated sabotage. This kind of HIO could be supported in the information domain by a pre-planned information campaign. Such an operation can paralyse entire nations and decision-making in the EU and NATO.

The emerging threat landscape introduces a very serious vector: pre-planned and well-coordinated cyber and physical sabotage carried out by skilled state actors. While it is impossible to eliminate every risk associated with such threats, increased investment in redundancy and recovery would naturally improve system security. The EU's Critical Entities Resilience (CER) Directive (Directive (EU) 2022/2557) provides a common framework to improve common understanding and the private sector's willingness to invest in resilience.

These examples from the infrastructure domain can be extended to other domains, such as public administration, economy or military defence.

High impact operations (HIOs) are hybrid threat operations intended to inflict recovery times. For example, in the event of power grid failure, systemic failure results from a coordinated, gradual build-up.

At the strategic level: rise of intensity to hybrid warfare

At the strategic level, several studies conducted since 2022 show that hybrid attacks against EU MS have intensified (Baumann et al., 2025; Burrows, 2025; Gurcov, 2025; Jones, 2025; Messmer et al., 2025). According to the foreign ministers of France, Germany, Italy, Poland, Spain and the United Kingdom, 'Moscow's escalating hybrid activities against NATO and EU countries are also unprecedented in their variety and scale, creating significant security risks' (German Federal Foreign Office, 2024).

The rise in intensity has also been assessed by the EU, which recognised an 'intensifying campaign of hybrid activities against the EU, its Member States and partners', revealed by and an 'increasing number of a broad range of activities' (Council of the European Union, 2024). This reveals from Russia 'broader, coordinated, and long-standing hybrid campaigns aimed at threatening and undermining the security, resilience and democratic foundations of the EU, its Member States and its partners', which are 'further escalating since the beginning of the war of aggression against Ukraine and highly likely to persist in the foreseeable future' (Council of the European Union, 2025).

Analysts and scholars identify two parallel trends: one domain dependent and one tool dependent. First, reports indicate an increased intensity across multiple hybrid threat domains, such as the political (Popescu-Zamfir, 2025), diplomatic (Lafont

Rapnouil, 2024), informational (Audinet et al., 2024; Rogozińska, 2026), cyber (Charter of Trust, 2025; Dyner, 2023), infrastructural (Dobbinga, 2025; Edwards et al., 2025), intelligence (Wiseman, 2025) and military defence domains (Khan, 2025; Bayer et al., 2026). Second, more offensive tools have emerged within the EU, including assassination plots (Madhani et al., 2024), arson attacks (Campbell et al., 2025; Sytas, 2025; Whitehead, 2025), flammable parcels sent by plane (Weiss et al., 2025), the jamming and spoofing of global navigation satellite systems (Höller, 2025; Martisiute, 2025), drones flying over military bases and nuclear weapons facilities (France 24, 2025; Salisbury, 2025) and penetration of EU territory by hostile military assets (Barbu et al., 2026; Khrebet, 2024; van den Berg et al., 2025).

Many analysts and scholars use the concept of hybrid warfare to qualify the situation (Baumann et al., 2025; Beznosiuk, 2025; Edwards et al., 2025; Messmer et al., 2025; Pabriks, 2026; Rekawek et al., 2025; Shahbazov, 2025; Stijnman, 2025). On the policy side, the concept of hybrid warfare has been endorsed. EU MS government and state officials use the concepts of 'hybrid warfare' or 'hybrid war' to qualify the situation (AFP/Euractiv, 2026; Chancellery of the Prime Minister of the Republic of Poland, 2025; French Presidency, 2024; LSM English, 2025; Office of the President of the Republic of Lithuania, 2022; Starcevic, 2025; Vasques, 2025; Yle News / STT, 2025).

At the EU level, the European Parliament, the European Commission and the European External Action Service employ the concept (European Commission, 2024, 2026a; European External Action Service, 2026a, 2026b; European Parliament, 2024, 2026). The President of the European Commission stated, unequivocally 'These incidents are calculated to linger in the twilight of deniability. This is not random harassment. It is a coherent and escalating campaign to unsettle our citizens, test our resolve, divide our Union, and weaken our support for Ukraine. And it is time to call it by its name. This is hybrid warfare' (European Commission, 2025a).

Russia, which operates extensive hybrid threat operations against EU MS and is 'preparing countermeasures against NATO in Baltics' (Interfax, 2025), poses, according to the High Representative of the Union for Foreign Affairs and Security Policy / Vice-President of the European Commission (HR/VP), 'an existential threat' to EU security (Reuters, 2025a).

As Russia escalates further its hybrid threat operations (Siebold, 2026), NATO, the EU and Member States' defence and intelligence institutions have underscored the risk of direct military confrontation (Albertini, 2025; Allison, 2025; Dunlop, 2025; European External Action Service, 2025a; Gardner et al., 2025; Jochecová, 2025; Ngendakumana, 2024; Telegraf, 2025).

*The European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE) defines **hybrid warfare** as 'a subset of hostile activities against a state, falling under the category of hybrid threats but representing an escalated phase. These activities may also involve military means and the use of chemical, biological, radiological, and nuclear (CBRN) threats, marking a shift from under-detected or unattributed activities to overt coercion. Hybrid warfare represents the "hard end" of the escalation spectrum of hybrid threat activity' (Hybrid CoE, n.d.).*

Figure 3 shows how escalation increases from low intensity to hybrid warfare. It also depicts how strong deniability at low intensity levels decreases as the intensity escalates, while hostile operations and strategies become more and more evident.

Typically, low-intensity hybrid threats are highly deniable, but escalation reduces deniability as intensity rises. However, while the denial generally decreases as intensity increases, hybrid threat actors still deny their involvement despite intensity rising, but with less credibility as their implication appears more evident. Substantial efforts are needed to conduct HIOs covertly and preserve deniability. In both cases (low- and high-intensity hybrid threats), attribution is challenging for different reasons: the difficulty in identifying and determining the source or the fear of further escalation.

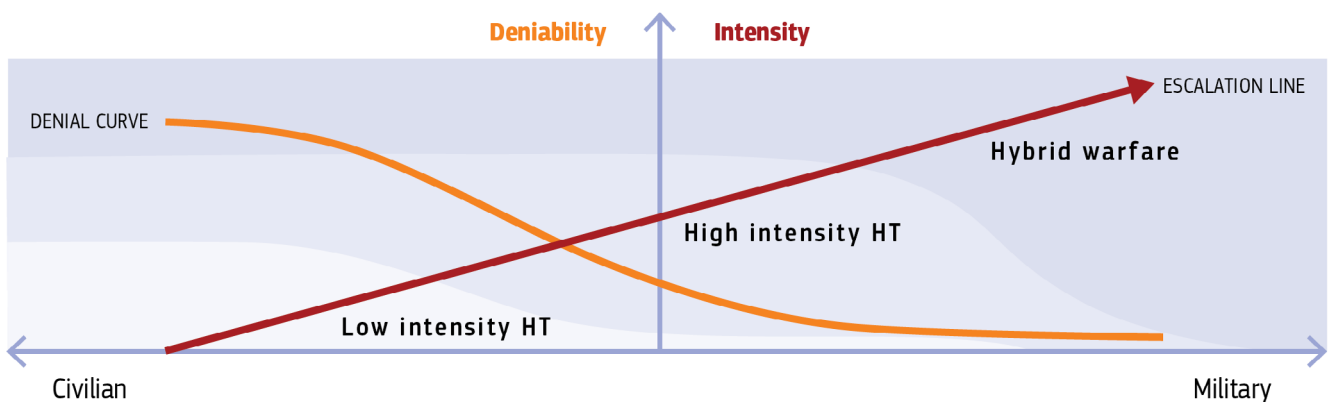
It is therefore necessary to prevent Russia from further escalation. Beyond enhancing resilience, a credible deterrence strategy is required (Monaghan et al., 2019) to ‘win the war before the war’ (Burkhard, 2021). Political resolve and decisive actions

should be employed to deter hybrid threat operations against Europe through reactive responses.

Any collective weakness or hesitation in this regard would be interpreted as not only permission but incitement to escalate further (Greene et al., 2026). Europe should therefore pursue a dual-track strategy to deal with adversaries: playing the long-term competitive game with strategies to structurally restrain the adversary, while applying a combination of resilience and deterrence measures to counter hybrid threats in the short term.

This report proposes a comprehensive strategy at the strategic level based on a combination of resilience and deterrence focusing on the short-term track.

FIGURE 3
Multiple exploitation of cascading effects



Source: EU

More on the new threat landscape

■ **Looking forward.** In a context of increased intensity, anticipation allows to derail hostile actor's strategies, particularly as it conceives and exploits cascading effects.

■ **Intelligence.** Democracies must improve the intelligence cycle to enhance detection across all hybrid threat domains and better determine the political end goals of hybrid threat operations. This would also support decision-makers in attribution. Horizontal cooperation, including under the European External Action Service's (EEAS) Single Intelligence Analysis Capacity (SIAC) is essential. The Intelligence College in Europe contributes to this effort by fostering a common strategic culture and bridging the capabilities of different EU MS intelligence services (Intelligence College in Europe, n.d.).

■ **Cognition.** At the political level, better information is required to refine cognitive systems, ensuring they remain uncontaminated by adversarial disinformation or propaganda. This approach helps mitigate cognitive biases rooted in historical, ideological, or calculative perspectives. It also emphasises collaboration with independent actors (academics, think tanks, individuals) who operate free from undue influence, sympathy, alignment, financing, or direct collusion with the adversary.

■ **Societal cohesion.** The deteriorating threat landscape combines increasing external pressure and subversive agitation within democracies, potentially triggering mechanisms of low-spectrum conflict (Theron, 2023). Societal cohesion, often neglected in liberal democracies, must withstand complex cognitive warfare (Hoffman, 2025), for instance on the model of Sweden's Psychological Defence Agency (Swedish Psychological Defence Agency, n. d.).

■ **Active and passive defence.** Current challenges necessitate the development of passive but also active defence measures across all domains. These measures are crucial for protecting the population and integrating them into a comprehensive whole-of-society resilience approach.

■ **Technology.** On one hand, there is intense competition for technologies, intellectual property rights, markets, and strategic resources. Even non-state actors are striving to achieve technological advancements, particularly in weaponry and cyber capabilities. On the other hand, low-tech strategies are emerging as a significant trend. These strategies are not confined to non-state actors but are increasingly adopted by states seeking to optimise the cost-benefit ratio of their operations.

■ **Political resolve.** Hesitation, delays, or indecision not only undermine the effectiveness of counter-strategies but also send a counter-productive message that may provoke further escalation. Addressing the evolving threat landscape necessitates prompt, clear, and decisive attribution.

■ **Spaces.** The civic space and the services space could and should be more associated to the governance space's countering strategies. Whole-of-society is the best asset of democracies and should be fully employed.

■ **Escalation management.** A new approach is needed to contain hybrid warfare, integrating deterrence. An advanced multi-domain strategy is essential to counter the escalating threats faced by Europe. This system should incorporate advanced anticipation of operations, active defence during attacks, and robust reactions to increase the cost of hostile behaviours.

1. PROACTIVE ANTICIPATION

The rapid rise of hybrid threat operations against EU MS requires, in line with the European security ecosystem on threat assessment, a review, adaptation and strengthening of Europe's response. Therefore, it is imperative to anticipate attacks more effectively, enhance resilience and apply deterrence specifically to hybrid threats. Resilience and deterrence must be conceived together and should anticipate future hybrid threat operations in order to prevent or absorb them.

Innovative attacks lie at the very core of hybrid threats, especially as these threats intensify. They encompass anticipatory planning, technological developments, new methods, combinations of actors, disruptive timing, cross-domain patterns and the exploitation of cascading effects. When resilience capacities become effective, adversaries adapt and attempt to bypass them; consequently, anticipating the development of future attacks plays a vital role in countering them.

Observation is essential, and foresight calls for a range of techniques such as technological foresight, horizon scanning and scenario building. Different 'traditions' exist depending on the institutional context: intelligence, police, border guards, the military or even sectors not traditionally linked to security and defence. EU MS intelligence services have their own protocols, and the EU possesses an integrated intelligence analysis mechanism in this domain: SIAC.

JRC's EU Policy Lab also proposes the European Strategy and Policy Analysis System, or ESPAS (European Strategy and Policy Analysis System, n.d.),

a horizon-scanning project that studies foresight and anticipatory governance. Domain-specific or cross-domain cooperation, for example the network of Information Sharing and Analysis Centres (EU ISACs), also improves preparedness. Beyond EU institutional mechanisms, Hybrid CoE's output facilitates improved threat foresight and anticipation. Integrating a coherent and comprehensive approach to foresight and anticipation into counter-hybrid threat strategies is therefore paramount.

Proactive anticipation, especially in security and defence, should be connected to capability-driven research and innovation processes. Identified future threats, vulnerabilities and operational scenarios should be translated into capability needs and research and innovation priorities, followed by the development, testing and validation of solutions with relevant practitioners, public authorities, critical entities and other operational end users. Where appropriate, this process should also facilitate subsequent investment, procurement, deployment and operational uptake.

The strategic autonomy perspective could also be broadened beyond the defence industrial base to cover the wider EU civil security and security technology ecosystems. Doing so would mean the following are included: trusted European capabilities for detection and situational awareness, secure communications, artificial intelligence (AI) and data analysis, cyber resilience, the protection of critical infrastructure, autonomous systems and the continuity of essential services. Critical dependencies in components, software, data infrastructure and supply chains could also be identified and reduced.

1.1 Operationalising resilience

Since 2016, resilience has been at the heart of the EU's policy on hybrid threats and has already been reinforced by EU institutions and Member States to withstand foreign and domestic pressures linked to hybrid threats. The EU 2020 Strategic Foresight Report defines resilience as 'the ability not only to withstand and cope with challenges but also to undergo transitions in a sustainable, fair, and democratic manner' (European Commission, 2020a).

The European Commission adds that resilience is 'the ability to face shocks and persistent structural changes in such a way that societal well-being is preserved, without compromising the heritage for future generations' (European Commission, n.d.).

In practice, this refers to a society's ability to function autonomously while under stress. It requires the development, adaptation and preservation of a reliable system, linked with like-minded partners, that can 'prevent, protect against, respond to, resist, mitigate, absorb, accommodate and recover from incidents' (European Parliament and the Council of the European Union, 2022; European Union, 2024).

The Niinistö report, *Safer Together: Strengthening Europe's civilian and military preparedness and readiness*, confirmed 'the urgency for the EU to step up its preparedness and resilience against the full spectrum of hybrid threats' (Niinistö, 2024, p. 103). The following year, the 'White Paper for European Defence – Readiness 2030' invited EU actors to address 'growing hybrid threats' (European Commission, 2025b).

Additionally in 2025, the 'EU Preparedness Union Strategy' listed among its key actions bolstering the resilience of European societies and the need to reach out to Europe's partners (European Commission and High Representative of the Union for Foreign Affairs and Security Policy, 2025). Published the same year, 'ProtectEU, a European Internal Security Strategy,' also foregrounds this concept (European Commission, 2025c).

Political declarations have likewise urged the EU to improve resilience against hybrid threats by enhancing absorption and recovery capacities. The Council of the European Union's 2022 conclusions explicitly call for greater societal resilience. In this context, the creation of the European Coalition for

Civil Preparedness and Resilience by an expanded group of countries underscores the need for 'better prepared and resilient societies' across the continent (Government of the Netherlands, 2025).

The total defence model adopted by several Baltic and Nordic states, with a whole-of-society security approach, further supports the demand for stronger societal resilience (Baltic Assembly, 2023; Nordic Defence Cooperation, 2024; Latvian Ministry of Foreign Affairs, 2025).

The Lublin Triangle countries ⁽⁵⁾ have echoed this sentiment (President of the Republic of Poland, 2021). The Weimar+ format ⁽⁶⁾ also called for 'enhancing resilience to cognitive warfare and hybrid threats in Europe, also through the relevant EU mechanisms, and promoting the resilience of our societies' (German Federal Foreign Office, 2024).

Finally, the Niinistö report advocates 'increasing the EU's resilience by tackling vulnerabilities and strengthening its capacity for damage mitigation' (Niinistö, 2024, p. 23).

At the national level, international cooperation through the security ecosystem is crucial for sharing best practices that boost collective resilience. For example, the crisis preparedness documents produced by the following European countries aim to improve collective resilience within the civic space:

- Estonia, *What To Do in a Crisis Situation – Be prepared!* (Päästeamet - Estonian Rescue Board, 2022),
- Finland, *Prepared People Cope Better* (Finnish Ministry of the Interior, 2024),
- France, *Tous responsables* (French Government, 2025),
- Latvia, *What to Do in Case of a Crisis* (Ministry of Defence of the Republic of Latvia, 2022),
- the Netherlands, *Prepare for an Emergency Situation* (Dutch National Coordinator for Counterterrorism and Security, 2025),
- Norway, *How you can play your part in Norway's emergency preparedness* (Norwegian Directorate for Civil Protection, n.d.),
- Poland, *Get Ready! Guide for crisis and war* (Polish Government Centre for Security, 2022),

- Sweden, In Case of Crisis or War (The Swedish Civil Contingencies Agency, 2024).

In accordance with identified needs and the following pattern, the operational measures for enhancing resilience are presented in Annex 1 of this report.

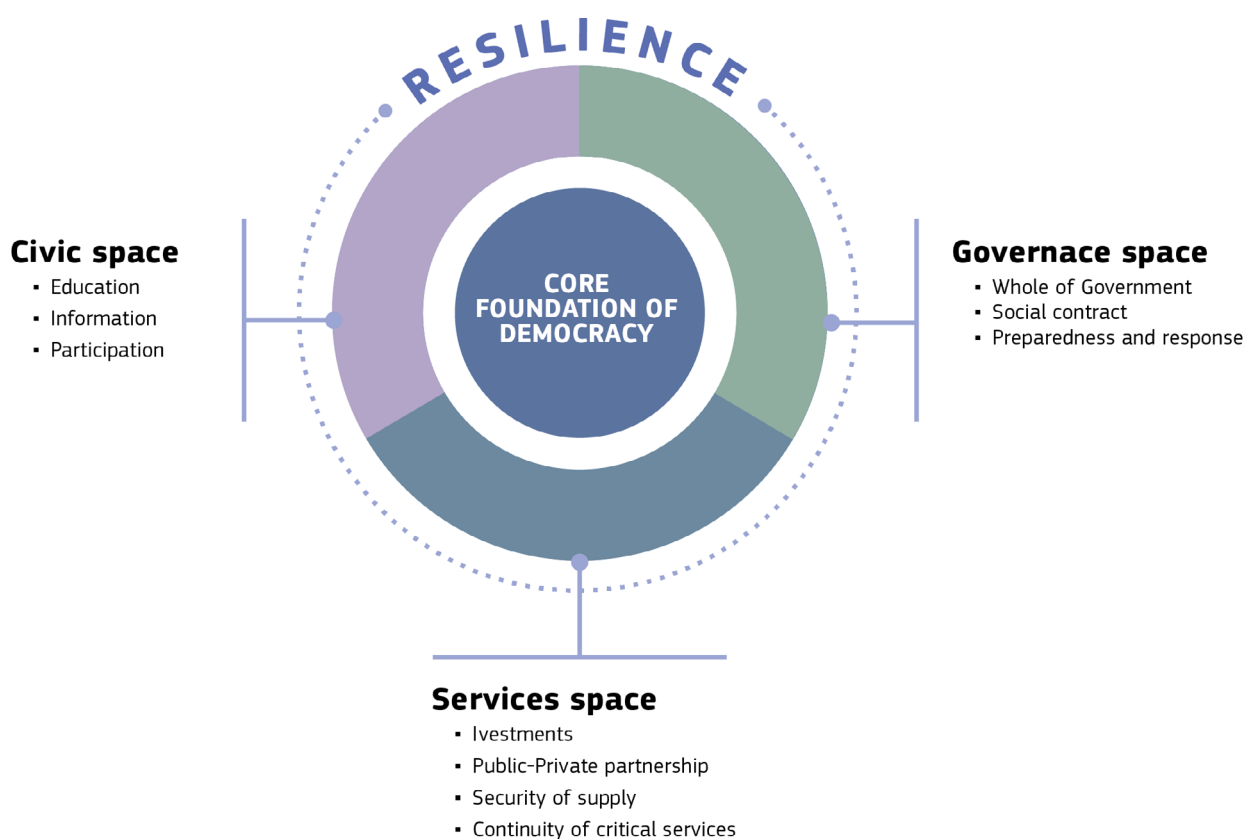
Figure 4 shows how the three spaces –civic space, governance space and services space – constitute natural frameworks to operationalise resilience based on the core foundations of democracy.

1.2. Introducing deterrence

As hybrid threat operations have expanded, enhancing resilience has become increasingly pressing as a means to counter them. The EU's approach to resilience against hybrid threats is primarily focused on defensive capabilities and systemic recovery. While vital, resilience alone cannot mitigate growing threats; it must be complemented by efforts to actively shape adversaries' perceptions and strategic calculus.

FIGURE 4

Operational resilience against hybrid threats



Source: EU

(5) Lithuania, Poland and Ukraine.

(6) France, Germany, Italy, Poland, Spain, the United Kingdom and EU representatives.

More on resilience

- Resilience does not depend on any single actor.
- A whole-of-society resilience model has been widely accepted by Member States, yet its practical implementation still falls short of the demands posed by hybrid warfare scenarios.
- Europe needs to strengthen preparedness for an increase in intensity from hybrid threat actors; a more resilient EU is urgently needed across all domains.
- Resilience should adopt an all-hazard approach to hybrid threats, concentrating on prevention, protection, ability to respond, resistance, mitigation, absorption, accommodation and recovery to ensure and maintain the continuity of government, continuity of operations, business continuity, key assets, essential services and vital functions.
- Resilience concerns every layer (international, national and local); and each citizen must be empowered to face disruptions to public and private services, including from high-impact events.
- Resilience-by-sector programmes could be launched in every Member State, respecting the complementarity of spaces and integrating short-, medium- and long-term strategies.
- Resilience measures must be flexible enough to adapt to evolving circumstances, especially when adversaries regularly change their tactics, combine multiple domains, innovate or exploit timing.
- The civic space is exposed on two fronts: unpreparedness for service disruption and vulnerability to hardened conflict. As a result, civic space's resilience differs markedly between Member States. It is therefore essential to raise awareness, preparedness and citizen involvement in defending democracies.
- The civic space is exposed on two fronts: unpreparedness for service disruption and vulnerability to hardened conflict. As a result, civic space's resilience differs markedly between Member States. It is therefore essential to raise awareness, preparedness and citizen involvement in defending democracies.
- Trust is a vital component of resilience building, fostering mutual assurance, confidence, closer cooperation and communication. A lack of trust can increase social polarisation, create inefficiencies, result in missed opportunities and hinder the implementation of resilience measures and inter-agency collaboration.
- International, civilian, military and civil-military cooperation through the European security ecosystem is essential for coordinating strategies and operations at the regional, European and global levels. The EU supports this through mechanisms such as the Union Civil Protection Mechanism (UCPM) (European Commission, 2026b) and the Military Planning and Conduct Capability's Rapid Deployment Capacity (EU RDC) (European External Action Service, 2025b).

The need for ‘going beyond resilience’ has long been recognised as ‘a necessary building block’, but ‘nevertheless insufficient when it comes to deterring Russia from unwanted acts’ (Bach Nyemann et al., 2018, p. 2). In 2020, Hybrid CoE produced a hybrid deterrence playbook, asserting that ‘hostile actors must be denied the space to operate’ (Keršanskas, 2020a).

In 2025, the Director of the European Union Institute for Security Studies (EUISS) warned that ‘the time of hope and illusion is really over now’ and that ‘resilience alone is not enough in the hybrid war with Russia’ (Everts, 2025). As hybrid threat operations intensify, the absorptive capacity of resilience becomes increasingly limited. Democratic societies are therefore more heavily impacted; deterrence is lacking, and hybrid threat operations even ‘undermine the foundations of deterrence – capability, credibility and communication’, obliging European democracies to ‘restore’ credible deterrence (Monaghan, 2022, p. 5). Failing to actively deter hybrid threat operations is therefore perceived as a weakness by both state and non-state adversaries.

The Niinistö report underlined the EU’s need for ‘outsmarting malicious actors to deter hybrid attacks’ in order to address ‘the increasingly brazen and aggressive nature of hybrid activities by external actors, in particular, but not only Russia’ (Niinistö, 2024, pp. 102–103). The E6/EU likewise affirmed the necessity ‘to address rising threats to security and meet the requirements to deter and defend across all domains in the Euro-Atlantic area’, specifically highlighting the need for ‘detering Russia’ (German Federal Foreign Office, 2024).

1.2.1. Why deterrence is essential to counter hybrid threat operations

Although the practice dates back to antiquity, the concept of deterrence was substantially expanded in the mid-20th century with the advent of nuclear strategy. After the World Trade Center attacks on 11 September 2001 in the United States, deterrence theory addressed terrorism and irregular warfare, a movement called ‘fourth wave’ in research, the first three waves relating to the rise of the atomic age, systemisation and real-world issues (Adamsky, 2023a; Knopf, 2010).

In this context, the adversary was no longer a state situated outside the deterring country’s perimeter but a non-state actor, prompting a shift towards a more population-centred approach as societies

themselves became the primary battleground of irregular warfare (Gray, 2006; Kitzen et al., 2021).

Deterrence is the ability to dissuade an adversary from launching an attack by demonstrating that the risk of severe consequences outweighs any potential gain.

Consequently, deterrence theory has continued to develop (Knopf, 2010) and adapt to increasingly dynamic and complex environments, including hybrid threat operations (Wigell, 2019). The most relevant conceptualisation for hybrid threats emerged when deterrence began to be applied to ‘grey-zone’ conflicts – a development sometimes described as a ‘fifth wave.’ Some scholars argue that the boundary between the fourth and fifth waves is indistinct (Adamsky, 2023b, pp. 9–12), while others contend that hybrid threats present unique challenges because of their multi-domain and cross-domain nature and their exploitation of complexity and ambiguity (Monaghan, 2022).

The prerequisites for effective deterrence are comparatively straightforward. Franck Hoffman describes it as ‘an exercise in interactive perception management that presumes clarity about the character of the geostrategic contest, and rationality in an opponent’s decision-making process. Deterrence is a perception about credibility and capability, and presumes a thorough understanding of competitors and their thresholds and decision calculus’ (Dunlap, 2022).

The EU’s multifaceted capabilities – regulatory, economic, innovative and normative – enable it to build a sophisticated deterring security ecosystem. Europe should, in this respect, ‘take account of and apply the power of financial pressure, of diplomatic pressure, of commercial pressure and not least of ethical pressure to weaken the opponent’s will’ (Liddell Hart, 1991, p. 322).

1.2.2. Primary concepts of deterrence

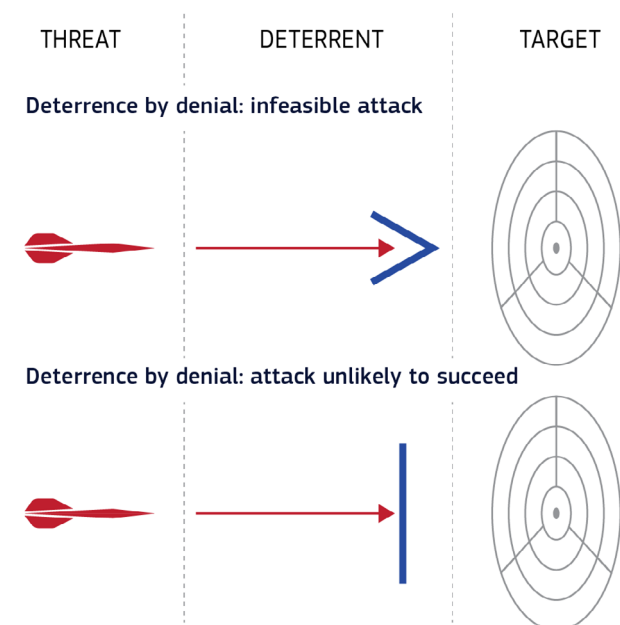
Classical deterrence theory seeks to prevent attacks by shaping an adversary's cost-benefit analysis. Accordingly, deterrence relies on two fundamental mechanisms: deterrence by denial and deterrence by punishment (5). Both concepts stem from classical deterrence theory, which underpins our understanding of how influencing an adversary's decision-making can avert aggression (Snyder, 2016).

1.2.2.1. Deterrence by denial

Deterrence by denial involves demonstrating the capacity to render an attack 'infeasible or unlikely to succeed' (Mazarr, 2018, p. 2), thereby reducing the adversary's incentive to act. Making an attack infeasible works by blocking it – a 'bulwark' strategy (Brands et al., 2024) – or by making it unlikely to succeed – which links denial to resilience (effect avoidance) (see Figure 5).

FIGURE 5

Two ways to exert deterrence by denial



Source: EU

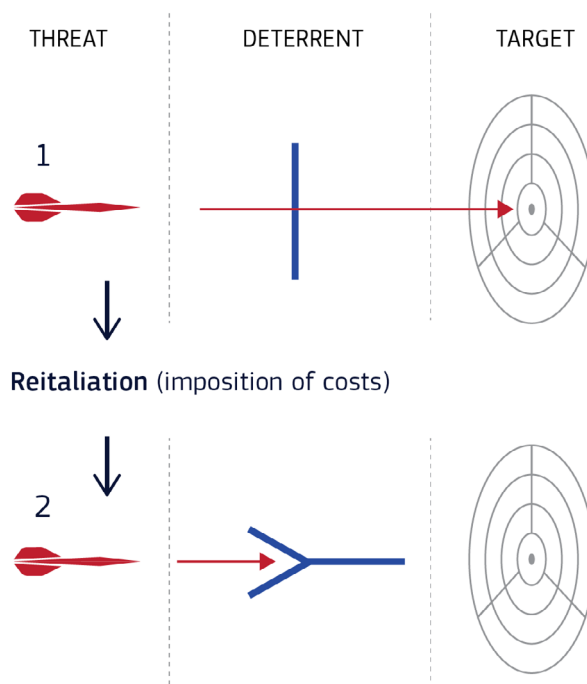
1.2.2.2 Deterrence by punishment

Deterrence by punishment involves imposing costs that outweigh any potential benefits of aggression, ensuring that the adversary perceives retaliation as unacceptable, as its capabilities would be degraded in the long term (Keršanskas, 2020b).

In the context of hybrid threat operations, this approach requires attribution before a reactive response is launched (see Figure 6). Only a clear precedent of retaliation can convince a hostile actor that the strategic resolve of its opponent will cost more than the attack could ever deliver. Schelling (1980, p. 189) explains, indeed, that deterrence by retaliation implies, to be effective, that "one must threaten that he will act, not that he may act, if the threat fails".

FIGURE 6

Principle of deterrence by punishment



Source: EU

Nevertheless, hybrid threat operations have largely evaded deterrence so far and risk eroding it altogether. As Popescu (2015, p. 2) notes, 'the reason hybrid operations have been perceived as so worry-

(5) Here, the taxonomy of denial and punishment can be juxtaposed with the Russian taxonomy of 'fear inducement' (ustrashenie), which is deterrence by fear, and 'forceful deterrence' (silovoe sderzhivanie), which is deterrence by the limited use of force to shape adversarial behaviour (Adamsky, 2023a, p. 24).

ing is because it is feared that they might have an impact on the credibility of deterrence (...). Hybrid operations might indeed constitute a risky but effective means of circumventing NATO's Article 5, and simply strike at the heart of political solidarity inside NATO and the EU.' This concern is highlighted by the fact that 'Russia appears to be playing both below and, potentially, beyond the threshold of conventional warfare' (Popescu, 2015, p. 2).

*Ultimately, the **deterrence of hybrid threats** by denial or punishment depends on shaping adversaries' perceptions. By combining denial (which reduces the attractiveness of aggression) and punishment (which raises its costs), states can dissuade hostile behaviour and protect their strategic interests.*

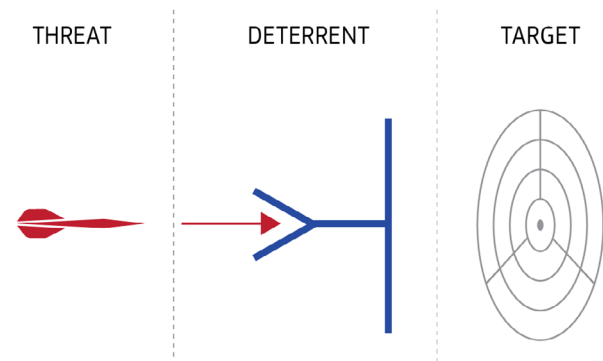
nuclear theory of mutual assured destruction, in which both sides face total annihilation.

When applied to hybrid threats, absolute deterrence means that any level of escalation the adversary is prepared to pursue will be met with an equivalent response – whether similar or dissimilar (horizontal escalation) – up to the point of political annihilation.

Democracies that wish to enforce absolute deterrence against hostile actors should send an unambiguous signal that any such offensive will inevitably lead to the aggressor's own destruction. Autocratic regimes' focus on their survival induces that they might prefer to refrain from decisions that could possibly result in their downfall (see Figure 7).

FIGURE 7

Absolute deterrence based on the anticipation of future operations



Source: EU

1.2.3 Secondary concepts of deterrence

Additional concepts can enrich the deterrence toolkit and prove useful for countering hybrid threats. The seminal work from Sean Monaghan at Hybrid CoE (2022) constituted a milestone in addressing multiple deterrence approaches to counter hybrid threats, a work on which this section has capitalised.

1.2.3.1 Absolute deterrence

Absolute deterrence seeks to prevent an attack from occurring altogether (Monaghan, 2022). A power balance threatens the attacker in advance with a strong response to its operation, echoing the

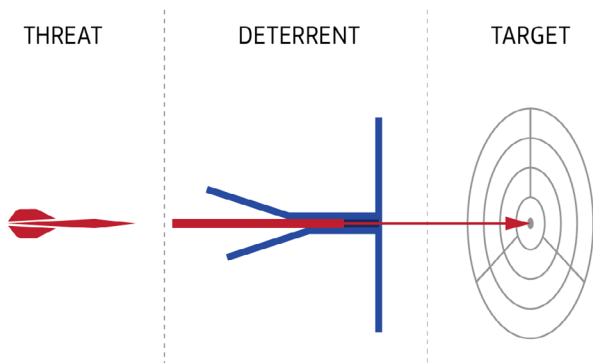
1.2.3.2 Restrictive deterrence

Restrictive deterrence, rather than attempting to prevent an attack entirely, seeks to limit the space available to perpetrators through incremental, compounding deterrent steps (Monaghan, 2022; Tor, 2017). By constraining the operational environment, the hostile actor is forced to conduct activities that are far smaller than originally intended.

This approach encourages early detection and a prompt response, thereby restricting the capacity to launch impactful hybrid threat operations. Moreover, the realist nature of restrictive deterrence supports business continuity while optimising overall resilience efforts (see Figure 8).

FIGURE 8

Restrictive deterrence, decreasing the intensity of the hybrid threat operation



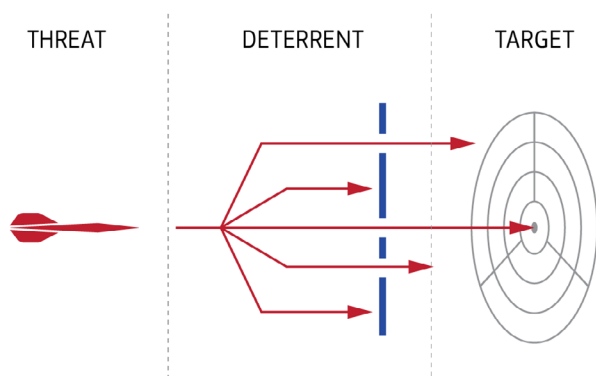
Source: EU

1.2.3.3 Cumulative deterrence

Similar to restrictive deterrence, cumulative deterrence focuses on measures that strengthen the overall position against the build-up of low-level attacks. It argues that individual operations are ‘rarely significant enough to justify the design of an entire deterrence posture to prevent them’ but offer the adversary the “snowball” effect of many low-level violations going unanswered over time’ (Monaghan, 2022, pp. 22–23).

FIGURE 9

Cumulative deterrence, limiting hostile operations to a tolerable minimum



Source: EU

Cumulative deterrence therefore seeks to constrain low-level threats so that the total impact remains under a controllable threshold. The approach aligns well with the conceptualisation of democratic resilience (Jungwirth et al., 2023, pp. 23–29). By limiting the frequency and severity of minor

attacks, cumulative deterrence reduces overall damage and helps maintain the continuity of governance, public services and civic space (see Figure 9).

1.2.3.4 Deterrence by disclosure

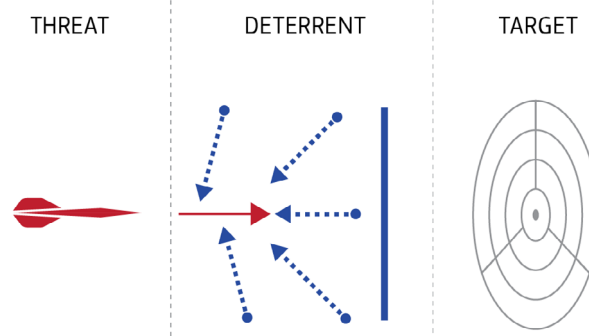
Deterrence by disclosure refers to the strategy employed by the United States prior to Russia’s large-scale invasion of Ukraine in 2022. The approach involved publicly revealing selected plans and preparations for conventional – and hybrid threat – operations.

The aim was to undermine the aggressor’s narrative, false-flag activities, offensive movements and overall conduct. ‘Naming and shaming’ diminishes the effectiveness of disinformation, weakens aggressor’s political standing and increase diplomatic pressure.

Described as an ‘intelligence revolution’ (Zegart, 2022), the marriage of secret intelligence and public diplomacy (Dylan et al., 2022) exposes adversarial fragilities and uncertainties (Edelman, 2022; Marleku, 2025). By using intelligence to produce a strategic effect (Huminski, 2023), deterrence by disclosure can form a component of a broader deterrence strategy (see Figure 10).

FIGURE 10

Deterrence by disclosure, publicly revealing hybrid threat operations at an early stage to undermine them



Source: EU

1.2.3.5 Deterrence by stratcom

As demonstrated by the NATO Strategic Communications Centre of Excellence, strategic communications or ‘stratcom’, can play a decisive role in countering hybrid threats (Heap, 2021).

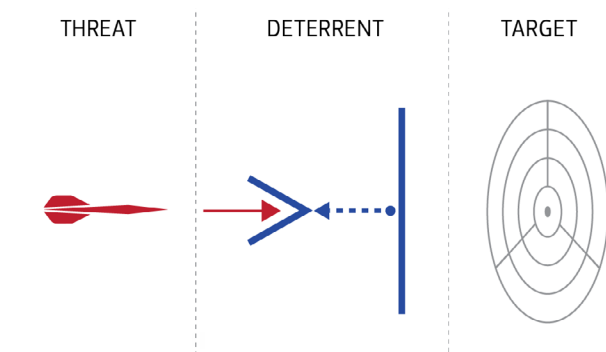
1. Proactive anticipation

What we say or do or choose not to say or do conveys a message. Actions, words and images shape audiences' perceptions and influence their decision-making, thereby producing strategic effects such as deterrence (Heap, 2021, p. 14). Deterrence is essentially an act of communication. By delivering strong, unambiguous verbal messages directly to an adversary, a defender can dissuade hostile behaviour (see Figure 11).

While ambiguity may be useful in other deterrence contexts, clarity is paramount here (Higgins, 2023), and '[s]tronger, clearer, and well-timed messages could be the difference between war and peace' (Michaels, 2025). Two conditions are essential. First, the defensive capabilities must be at least as robust as the message. Second, if the adversary nevertheless proceeds, they must be met with a decisive backlash. As Heap (2021, p. 17) notes, 'Credibility is the cornerstone of strategic influence, especially deterrence.'

FIGURE 11

Deterrence by stratcom



Source: EU

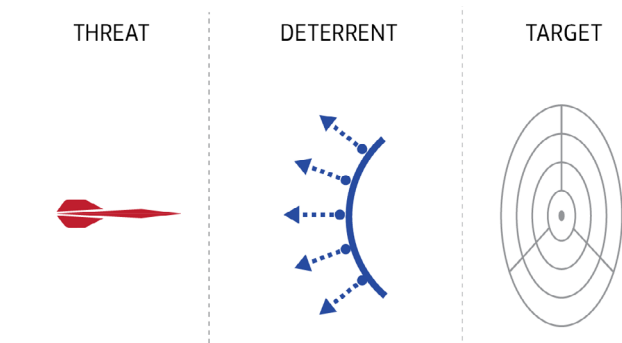
1.2.3.6 Integrated deterrence

Integrated deterrence, developed in the 2022 US National Defence Strategy, aims 'to develop, combine, and coordinate (...) strengths to maximum effect' (United States Department of Defense, 2022, p. IV). This form of deterrence seeks to create a psychological effect on the adversary, through strong resolve, thorough knowledge of the available assets and efficient inter-agency articulation. As the US Secretary of Defence explained, the idea 'is the right mix of technology, operational concepts and capabilities — all woven together and networked in a way that is so credible, flexible and so formidable that it will give any adversary pause' – adding that '[w]e need to create advantages for us and dilemmas for them' (Austin, 2021). Interesting lessons can be learned from it, such as allies'

'stakes, commitment, (...) credibility; their perception of their own ability to control escalation risks' (United States Department of Defense, 2022, p. 8) (see Figure 12).

FIGURE 12

Integrated deterrence, preventing an attack by preventively scaling multiple capabilities



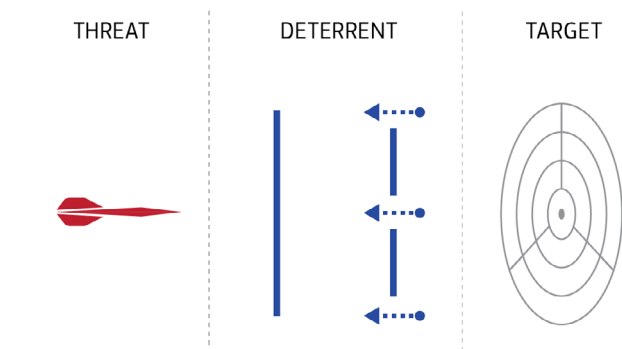
Source: EU

1.2.3.7 Internalised deterrence

Internalised deterrence, Freedman explains, can be embedded within society as a 'political process' (Freedman, 2004, p. 31). In practice, 'the act of deterrence may be no more than a hint here and a quiet word there, sufficient indication that the possibility of the offending act has been noted, and preparations are being made' (Freedman, 2004, p. 31). This presupposes that credible counter-capabilities have already been implemented, as noticed by the incidental concept of deterrence by capacity (Jensen, 2026), which can take decades but be most efficient (see Figure 13).

FIGURE 13

Internalised deterrence: hoarding dissuading capabilities to lower the need for strong acts of deterrence



Source: EU

1.2.3.8 Extended deterrence

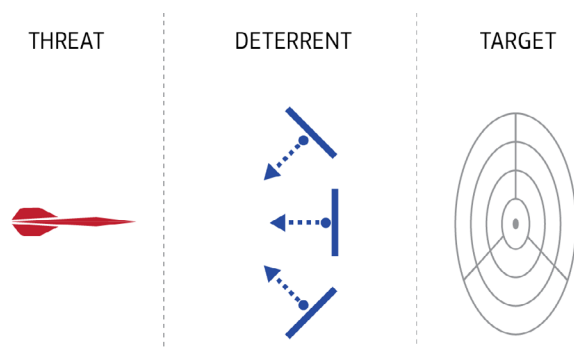
Extended deterrence is a guarantee by one state to defend another (see Figure 14). Strategic studies on nuclear deterrence introduced the illustrative notion of a ‘nuclear umbrella’, but the concept also applies to conventional and non-conventional threats. Extended deterrence is of major importance for international security; as Freedman (2004, p. 45) observes, ‘there would be few instances in which it could be asserted with confidence that B reconsidered an original intention to act in a particular way solely because of a conditional threat issued by A.’

While NATO and the EU can help states expand their military and economic statecraft capabilities, credibility and resolve become more challenging in alliances that require unanimity for decisions (Monaghan, 2022), noticeably in a complex international security environment (Stubb, 2025).

Collective deterrence may lack credibility for any ally if capabilities are not distributed so that the weakest members are protected with a high degree of certainty in the adversary’s mind.

FIGURE 14

Extended deterrence: collectively shielding an attacked ally



Source: EU

1.2.3.9 Deterrence by inducement

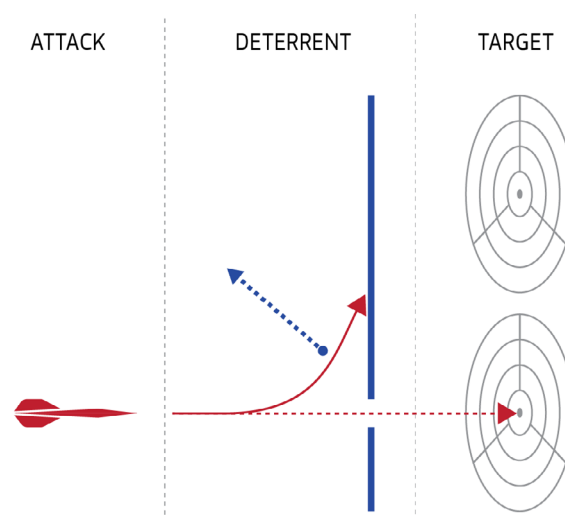
Deterrence by inducement relies on resilience, both in proactive anticipation and during active defence. Inducement may take the form of incentives (offering a benefit that outweighs the attacker’s original gain), entanglement (a third actor aligns with the desired outcome), diversion (applying technical or

human pressure), deception (using lures or bait to mislead the adversary), ruse (manoeuvring or camouflaging to conceal one’s true intentions) or forced deviation (arrest or kinetic action that halts the attack).

Channelling the impact towards less critical vulnerabilities can limit the overall effect of the operation (see Figure 15). However, the approach may be risky if the adversary discovers the inducement attempts, as this might enable it to exploit vulnerabilities.

FIGURE 15

Deterrence by inducement to deviate hybrid threat operations’ harmful trajectories to better defended area



Source: EU

1.2.4 Operationalising deterrence

Deterrence is a form of messaging directed at not only adversaries but also allies and third parties. The rapidly changing international security environment is highly complex, that is, ‘the number of interactions between components increases dramatically (...); this is where things quickly become unpredictable’ (McChrystal et al., 2015, p. 57).

Returning to an ex ante world is not feasible; Europe must leverage its numerous advantages more effectively through, for example, the following.

- Europe could create a ‘democratic security bubble’ by adopting a protective anti-access / area

Primary concepts of deterrence

Deterrence by denial:

preventing to perform a successful attack

Deterrence by punishment:

imposing sufficient costs to prevent future attacks

Secondary concepts of deterrence

Absolute deterrence:

Averting the attack by building capabilities in anticipation

Restrictive deterrence:

constraining the intensity of the attack to make it tolerable

Cumulative deterrence:

concentrating deterring efforts to limit the threshold of harm

Deterrence by disclosure:

exposing incoming attacks to sap the adversary's denial

Deterrence by stratcom:

signalling resolve and readiness to counter the attack

Integrated deterrence:

*displaying powerful deterring strength
Internalised deterrence: quietly setting up internal preparedness in case*

Extended deterrence:

strengthening collective security to dissuade the attacker

Deterrence by inducement:

incentivising the adversary to target the most resilient area

denial (A2/AD) ⁽⁶⁾ approach to hybrid threat operations across all domains in concert with allies. This approach induces collective action to address hostile operations through both denial and punishment and could protect Europe by reducing the overall damage to democratic societies.

- Hybrid threat operations targeting Europe are not limited to the continent; they are carried out globally, from the Arctic (Kertysova et al., 2023; Østhagen, 2023; Zysk, 2023) to Africa (Kremidas-Courtney, 2023), from Latin America (Baisotti, 2023; Hobbs et al., 2022) to the South Pacific (Brady, 2024; Grare, 2024). In response, as a global power, Europe should look to maximise its assets worldwide, including diplomatic, information and economic tools.
- Hybrid threat actors exploit links with third parties; therefore, involving those partner states and international organisations in a deterrence strategy is essential. Using incentives, whether they are positive (leveraging partnerships) or negative (secondary sanctions), can help isolate adversaries and cut off their resources.
- Since its inception, Hybrid CoE has compiled a corpus of studies on deterrence against hybrid threats with an operational dimension. The research covers specific domains – cyber (Pernik, 2021; Taddeo, 2018), disinformation (Keršanskas, 2021), economic (Shagina, 2022, 2024), infrastructure and military (Savitz, 2024) – as well as particular topics such as state proxies (Rauta, 2025). These studies can be used by domain practitioners to implement deterrence at the operational level, particularly when confronting adversaries: ‘a deterrent effect may be created by putting these interests at risk through threats of armed force, but also non-military measures, and can be reinforced by a variety of economic and political inducements and reassurances’ (Freedman, 2004, p. 59).

⁽⁶⁾ This concept in military defence originated by associating anti-access (limiting the arrival of capacities in a theatre of operations) and area denial (preventing freedom of action once capacities are operating in the theatre) (see Musland, 2021). The concept of A2/AD refers to a multi-domain strategy, mobilising multiple measures to contain the adversary's ability to conduct effective hostile operations.

- The assumption that an adversary could not or would not launch an attack can originate from misunderstanding its strategy because of cognitive biases. Cognitive biases can therefore undermine the formulation of effective deterrence strategies. Underestimating the opponent can become a principal cause of operational and strategic defeat that stems from cognitive biases at high administrative levels or within decision-making cabinets. Fact-based analysis, robust information sharing with allies, more horizontal exercises of power and transparent decision-making processes are ways to mitigate cognitive biases.
- Sophisticated deception strategies are employed by hostile actors to conceal their true intentions; these tactics should be addressed by countermeasures. These strategies leverage efficiency when they exploit existing cognitive biases. A fait accompli presented by an army mistakenly perceived as unbeatable, or the belief that creating commercial dependence poses no security risk, are deceptive elements that adversaries weaponise to facilitate hybrid threat operations against Europe. Consequently, deception shapes societal narratives, incapacitates decision-makers, facilitates hybrid threat operations and advances antagonistic interests.
- The assumption questioning the attacker's rationality should be considered with extreme prudence. All actors behind hybrid threat operations certainly follow different logics but must be regarded as highly rational, whether they are state or non-state entities (Bicchiari, 2009). Even when their strategies appear seemingly absurd to us, this does not render them irrational. Differences in strategic culture and tolerance for risk are sources of dangerous misunderstanding and strategic mistakes. The adversary should always be analysed thoroughly and deterred with the utmost determination.
- Deterrence against hybrid threat actors should form the core of escalation management. Inaction incites escalation, and nothing accelerates it more than allowing attacks to proceed without imposing seriously harmful consequences. Indeed, 'it is folly to imagine that the aggressive types (...) can be bought off – or, in modern language, 'appeased' – since the payment of danegeld stimulates a demand for more danegeld. But they can be curbed. Their very belief in force makes them more suscep-

tible to the deterrent effect of a formidable opposing force' (Liddell Hart, 1991, p. 359).

1.2.4.1. Deterrence against the weaponisation of cascading effects

Preventing adversaries from carrying out hybrid threat operations also involves countering the exploitation of cascading effects. In other words, dissuading hostile actors from extending an attack so that it causes further harm relies on deterrence. While deterrence by denial helps to make the exploitation of cascading effects infeasible, deterrence by punishment is the primary mechanism. If a robust retaliatory response imposes a sufficient cost after the initial operation, the adversary should be compelled to abandon any attempt to amplify the impact, rather than allowing the effects to become entrenched in the target society over the long term.

Achieving this requires that the governance sphere, supported by security services and civil-society actors, detect, identify and accurately assess the full scope of potentially harmful exploitations that may arise from cascading effects. This presupposes the ability to anticipate not only the potential secondary impacts but also the adversary's political, procedural, material, financial and human capacities to exploit them.

1.2.4.2. Deterrence to prevent High Impact Operations

An HIO creates an urgent need for robust, targeted deterrence, including deterrence by punishment, to prevent actors from getting away with their attack. As depicted in Figure 3, the deniability of an HIO is less credible due to the intensity and means of the operation, so even if the adversary denies it, as is in the nature of its hybrid strategy, attribution should be eased by the intensity of the operation, permitting retaliation.

Striking back decisively – and doing so complying with democratic standards – should exploit the vulnerabilities of autocratic regimes, imposing costs that are intolerable for the adversary and discouraging any future planning of HIOs.

The penalty that adversaries must face for attacking Europe should be unbearable enough to deter them from conducting further impactful attacks, and then, a fortiori, HIO. This fundamental principle must be applied not only within each individual domain but also as a comprehensive strategy, given the hybrid nature of the threat. Although attacks can be ambiguous – particularly in sectors such

as culture, intelligence or economics – it remains essential to act forcefully with decisive measures that demonstrate a clear resolve not to allow further operations to cause intolerable harm.

To contain the rise of intensity and deter HIOs, an incremental approach appears inadequate for two reasons:

1. its deterrent effect is limited, as step-by-step measures never impose a sufficient cost;
2. it supplies the aggressor with information and a window of time to adapt its tactics to the changing response.

Consequently, strong responses are necessary to surprise and destabilise the adversary, especially to counter HIOs.

1.2.4.3. Importance of collective security

Robust institutionalised and ad hoc cooperation mechanisms are essential to deliver deterrence, as they strengthen strategic reassurance, political legitimacy, international legality and economic stability. In this regard, many hybrid threat operations are precisely designed to weaken coalitions – first and foremost the EU and NATO but also other cooperative mechanisms. It is easier to reduce European states' collective strength and undermine their democratic systems once they are isolated.

As hybrid threat actors align, an efficient counter-strategy requires deterrence built on flexible yet strong international alliances, both within Europe and beyond. Because the international security environment is volatile and highly sensitive to political alignment, deterrence could be pursued as a multi-domain system of systems or 'teams of teams', linking different security ecosystem networks 'to achieve strategic – not just tactical – success' (McChrystal et al., 2015, pp. 128–130).

As Roberts (2019) notes, 'We want the adversary to believe that we have the political will to deny benefits and impose cost, even if it comes at a price to ourselves. (...) We will deter more effectively if we show our adversaries that we have partners who are ready to act with us, for example in imposing political, economic or other costs.'

The EU is a unique organisation that shares both challenges and capabilities, resulting in a high degree of goal alignment among its Member States. The EU has repeatedly supported Member States and external partners in repelling hostile hybrid threat operations.

Although each Member State holds the mandate to counter hybrid threats, many lack the resources and capacities required for proportionate retaliation, and all can benefit from effective extended deterrence provided by the bloc. Indeed, the EU possesses the distinctive capacity to enhance the deterrence strategies of its Member States by providing domain-specific and multi-domain countermeasures that leverage their ability to respond, individually but also collectively, to hybrid threat operations.

1.3. Articulating resilience and deterrence

1.3.1. Combining resilience and deterrence

Proactive anticipation means that deterrence as well as resilience work to avert attacks as far as possible through preventive measures. If an attacker nevertheless decides that an attack still yields a benefit despite denial and the risk of a costly response, resilience – already planned in advance – protects society from being seriously affected.

Proactive anticipation rests on four postulates:

1. deterrence and resilience are both necessary;
2. deterrence and resilience are compatible;
3. the two concepts can be combined to optimise strategy;
4. both must be conceived and implemented in anticipation.

Deterrence and resilience constitute a single system as they inevitably influence each other (see Figure 16). Enhancing resilience automatically strengthens deterrence, while a higher level of deterrence enables more robust resilience.

As Shagina (2024, p. 3) observes, 'calibrating the right pain threshold' requires understanding the amount of harm that society can absorb through resilience and the point beyond which hybrid threat operations must be deterred.

Beyond its strategic, anticipatory aspect, the combined system of deterrence and resilience also has a direct operational impact, shaping both the onset and conduct of hybrid threat operations.

More on deterrence

- *Historically rooted in the military sphere, deterrence could now be extended to a civil military cooperation framework. While deterrence is comparatively straightforward in the military domain, it can be applied to all other domains – including social, societal, informational and cultural spheres – even when the relevance of those domains is not immediately apparent. Therefore, the three spaces – governance, services and civic – should all be incorporated into deterrence strategies.*
- *Deterrence can be defined in doctrinal terms as actor agnostic, yet in practice it must be actor dependent both strategically and operationally. Because the threat landscape is highly specific, effective deterrence strategies need to be built on the most specialised expertise concerning each relevant actors and tailored to the particular dangers they pose.*
- *Deterrence against hybrid threat operations must consider the full although complex combination of actors (state and non state, foreign and domestic proxies), as well as their varied type of relations (operational cooperation, strategic support, exploitation of operations, antagonistic objectives but parallel anti-democratic narratives).*
- *Cooperation mechanisms should leverage the capacities of individual states; a strong coalition remains the most valuable asset for ensuring effective deterrence. An efficient European deterrence system must transform the theoretical concept of extended deterrence into a unitary, dynamic, adaptive and democratic security ecosystem, capable of anticipating and preventing HIO.*
- *While the material conditions for deterrence may be met, the real challenge often lies in securing sufficient political resolve. When decisiveness or a shared commitment is lacking, the effectiveness of deterrence is weakened, which encourages further aggression. As Jervis (2017, p. 58) notes: “Great dangers arise if the aggressor believes that status quo powers are weak in capability or resolve.”*
- *Deterrence relies on repetitive game theoretic dynamics; actors learn from past strategies and adapt to avoid repeated failure. Consequently, deterrence must anticipate an adversary’s future threats and adapt to counter tomorrow’s hybrid threat operations. Full use should be made then of deception, strategic ambiguity and disruption to dissuade the adversary to conduct its operations.*
- *Roberts (2019) identifies key assets for implementing an efficient deterrence strategy against hybrid threats: intergovernmental cooperation, resilience, capabilities, resolve, agility, coherence, communication of strengths, transparency and the avoidance of miscalculations.*

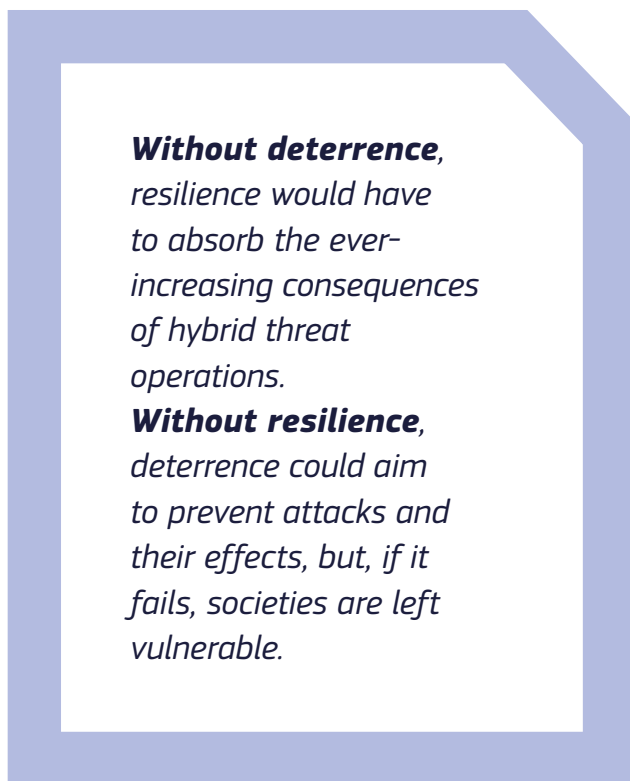


Figure 17 shows different situations where resilience and deterrence can be optimised: repelled or absorbed by resilience (deterrence by denial) or followed by the imposition of cost (deterrence by punishment). After several hybrid threat opera-

tions, the democratic defender proceeds to recover quickly and improve its trajectory, while conducting a reactive response against the attacker – a move producing a strong deterrent effect.

1.3.1.1. Requirements for combining resilience and deterrence

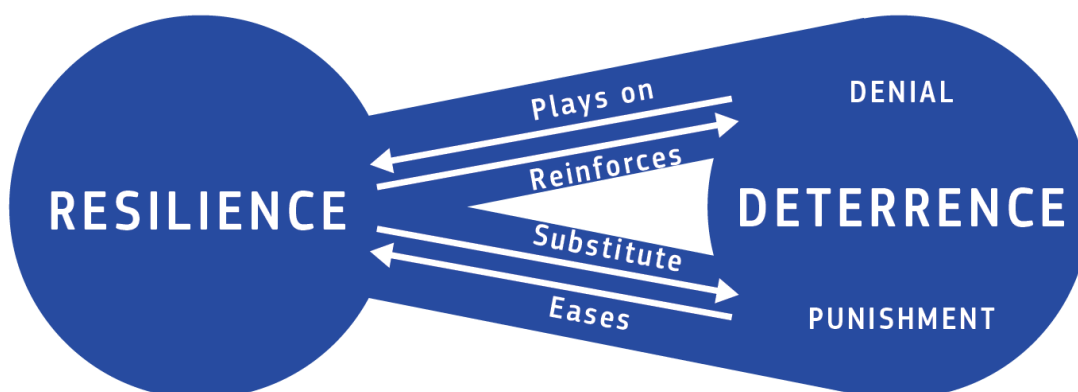
Ten operational requirements can improve proactive anticipation.

1. **Strategic depth.** Hybrid threat operations can impact societies to varying depths and degrees of visibility. Cognitive warfare, for instance, can run deep and over the long term. Some operations can also reactivate dormant or 'sleeper' campaigns, bringing them back into the public view. For instance, in the information sphere, the narrative that Moscow is the saviour of African nations revives a Soviet-era information operation that sought to exploit liberation movements, align newly independent states and turn them against the West.
2. **Integration of disruption.** Linearity follows a cause-and-consequence model, yet disruptions frequently break this pattern and catch security-defence apparatuses off guard. Such high-impact, low-probability events – often termed 'black swans' (Ducaru et al., 2019) – demonstrate the need to 'never discount or

FIGURE 16

The relationship between resilience and deterrence

Source: EU



Source: EU

1. Proactive anticipation

ignore the possibility or probability of folly, incompetence, and sheer bad luck' (Gray, 2008). A recent example is the drone campaign that swept across several European countries, shattering the status quo of European airspace security.

3. Complexity management. Hybrid threat operations are shaped by a multitude of variables: material elements such as resources and capabilities; social components, including individuals and groups; technological factors, like cyber tools, weaponry and transport; and networking aspects that span the social, societal and digital spheres. At the strategic level, these operations are combined in multi-domain campaigns that accumulate over time through cascading effects. It is a challenge to design an anticipation strategy based on resilience and deterrence, as this complexity requires enhanced analytical and public policy capacities.

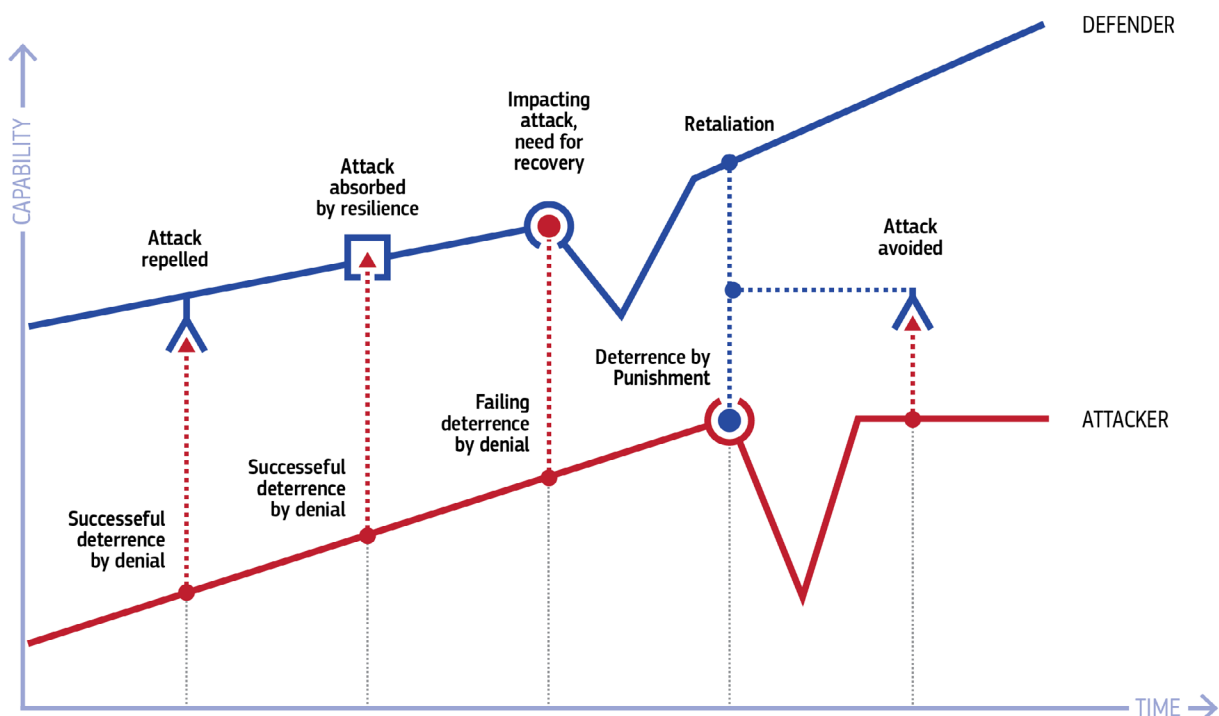
4. Questioning of certainties. Anticipation must challenge existing knowledge and avoid over-reliance on preparedness, which an adversary can readily identify and circumvent. AI can aid this by flagging low-level signals and exposing invisible links between events, actors or timings. Structurally, it is preferable to be

adaptable rather than adapted. For instance, intelligence that does not fit a preconceived pattern can prove valuable a posteriori.

5. Anticipation's implementation. Policy documents constantly stress the primary importance of anticipation, yet scaling up anticipatory measures and translating them into genuine change is particularly difficult, even for high-probability, high-impact scenarios, known as 'grey rhino' events (Atkins, 2021, pp. 440–441). Anticipation studies must therefore move beyond theory: their findings should be analysed and turned into concrete adaptations. For example, allowing disinformation outlets and personalities to operate openly or permitting military build-ups around the EU territory demonstrates a lack of anticipatory strategy. To avoid a gap between strategic analysis and operational readiness, anticipatory findings should be tested through experimentation, demonstrations, simulations and operational exercises. This should include iterative feedback from practitioners and end users, and the testing of interoperability, usability, scalability and resilience under realistic multi-domain conditions.

FIGURE 17

Possibilities of resilience and deterrence to counter hybrid threat operations



Source: EU

- 6. Adaptation celerity.** Studies and exercises on adaptation often prepare (t) based on past hybrid threat operations (t – 1) rather than on future scenarios. Then, they require time to reach decision-makers (t + 1), to implement them (t + 2) and to evaluate them (t + 3). By contrast, anticipation should follow a truly forward-looking process with rapid implementation. Mastering the agenda by anticipating hostile operations to adapt resilience and deterrence is essential. For instance, streamlining bureaucracy and accelerating administrative procedures would speed up operational adaptation.
- 7. Political resolve.** Strong will power is essential for adapting to future threats. This requires an excellent flow of information within the governance sphere and openness to the services and civic sectors. Decisive leaders who look far ahead and make forward-looking decisions help deter escalation.
- 8. Strategic decisiveness.** Anticipatory adaptation must be carried out with strategic decisiveness rather than following a mere tick-box approach, particularly in a context of increasing threats. Effective strategy optimisation relies on effect-based bottom-up recommendations, top-down leadership and cross-cutting coordination. This approach pushes for the continuous evaluation and adjustment of the anticipatory measures that have been implemented.
- 9. Whole-of-society approach.** Integrating the three spaces – governance, services and civic – into a comprehensive anticipatory strategy enhances the chances of deterring or absorbing future hybrid threat operations. When civic actors participate in anticipating hostile activity across the intelligence, information and cyber domains, society as a whole becomes more resilient and improves its deterrence capability.
- 10. Norms and entanglement.** The EU relies on useful regulatory norms, although these are undermined by the unregulated use of force (Hathaway et al., 2025). The concept of entanglement – that is, global interdependency with third parties – is also highly helpful for bringing third parties into deterrence efforts, although it requires long-term strategies. While secondary sanctions demonstrate a deterrence capacity linked to violations of international law, initiatives such as the Global Gateway provide the EU with valuable assets to improve resilience through entanglement.

1.3.1.2. Anticipating impact

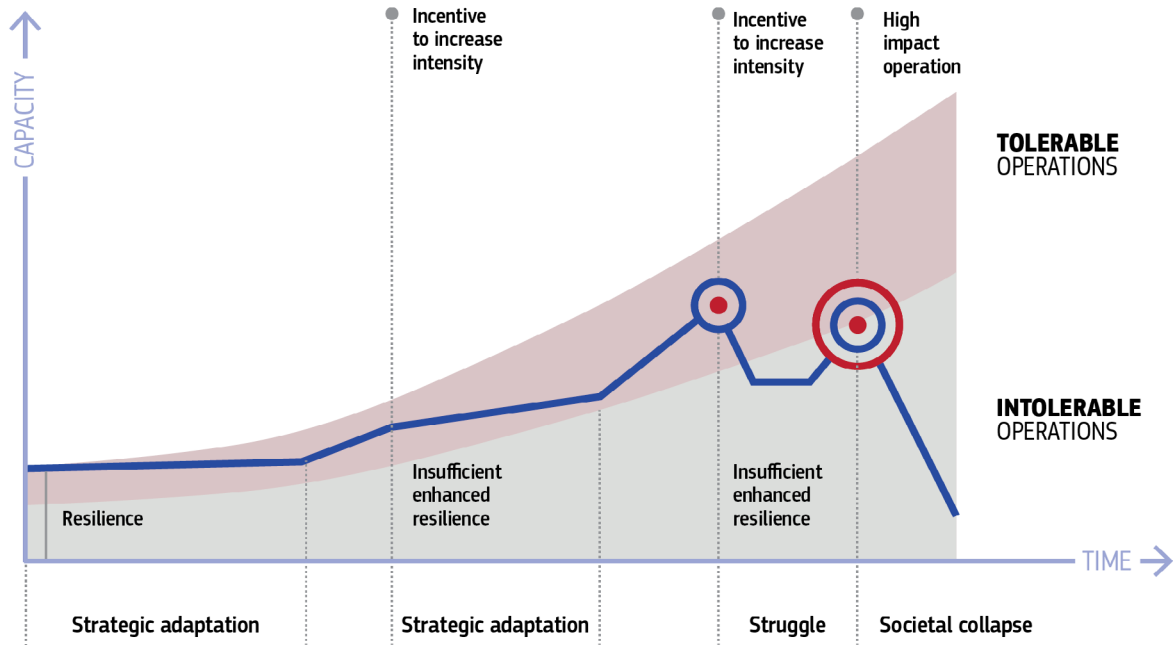
Proactive anticipation must consider the full range of hybrid threat operations. One way to understand these configurations is to combine impact and probability, a pattern that demonstrates that the interplay between deterrence and resilience must be tailored to each situation, as depicted in Table 1.

Anticipating hybrid threat operations requires taking the associated risks into account by assessing the available knowledge of those risks, addressing both the knowns and the unknowns (Jungwirth et al., 2023, p. 49). Specific recommendations can help to manage the issues of impact and probability.

- Assess the potential consequences of both inaction and action to support balanced decision-making when anticipating operations with different probabilities and impacts.
- Base decision-making protocols on inputs from practitioners, particularly intelligence analysts from specialised services; political decision-makers hold the mandate to decide but can be outpaced by technical considerations and complex chains of consequence.
- Introduce standardised assessments of strategic biases concerning adversaries in the recruitment and training of political, diplomatic, military and intelligence personnel at all levels.
- Regularly train practitioners to identify, resist and counter cognitive warfare techniques, thereby preventing cognitive biases regarding probability/impact analysis.
- Prepare for foreseeable and disruptive HIOs across all domains through inter-agency and inter-ally preparedness programmes.
- Educate about the specific risks and possible ways of addressing low-impact operations.
- Develop awareness programmes for the civic and services spaces that explain the various risks and outline concrete ways to build resilience and contribute to deterrence efforts.

FIGURE 18

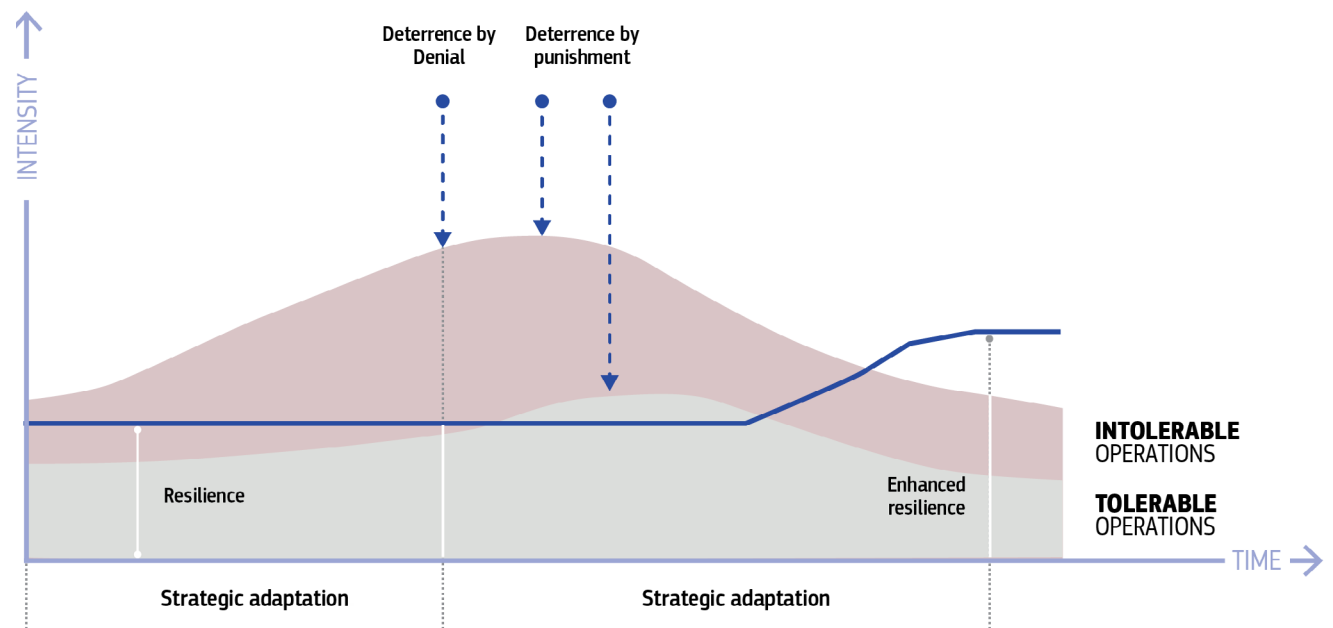
Societal collapse due to insufficient resilience and the absence of deterrence



Source: EU

FIGURE 19

Cumulated effect of deterrence and resilience on hybrid threat operations



Source: EU

Figure 18 depicts a counterexample where the defender runs after the attacker, insufficiently trying to adapt and eventually being strongly impacted by an HIO.

Figure 19 shows an example of how cumulating deterrence and resilience can contain the impact of hybrid threat operations.

as the tabletop EU–NATO Parallel and Coordinated Exercise (PACE) and EU–NATO Coherent Resilience (CORE) exercises. Other options, depicted in Table 3, can improve practitioners’ skills at all levels and also help integrate various actors from the services and civic spaces.

1.3.2. Proactive anticipation in practice

Deterrence and resilience must be closely coordinated from a very early stage at the strategic level. The success of a tailored security strategy depends on this upstream strategic coordination. Several practical anticipatory measures can help mitigate the ‘defender’s dilemma’ (Monaghan, 2022, p. 11). Table 2 shows how anticipation operates at the strategic and operational levels.

Based on a clear strategic/operational pattern as proposed in Table 2, the proactive deterrence–resilience capacities of the security ecosystem can be optimised through a range of exercises, such

TABLE 1
Different types of hybrid threat operations and possible proactive anticipation combinations

		IMPACT	
		LOW	HIGH
PROBABILITY	LOW	LILP: Absorbable operation with long-term campaign risks → Cumulative deterrence + Resilience	HILP (“black swan”): Disruptive high impact operation → Deterrence by denial + Restrictive deterrence + Deterrence by punishment + Resilience
	HIGH	LIHP: Absorbable with multi-domain cumulative risks → Cumulative deterrence + Deterrence by disclosure + Deterrence by denial + Resilience	HIHP (“grey rhino”): Foreseeable high impact operation → Deterrence by disclosure + Restrictive deterrence + Deterrence by punishment + Resilience

Source: EU

TABLE 2

Means to improve the proactive dimension of the deterrence-resilience system

STRATEGIC PROJECTION	Foresight Identify and confronting multiple possible futures and their desirability (European Strategy and Policy Analysis System (ESPAS))	Prospective Building from current trends to infer future attacks	Predictive Defining given situations that may occur in the future, regardless their probability, to determinate credible paths of events leading to them
OPERATIONAL ANTICIPATION	Adaptation Producing the necessary transformation to cope with incoming attacks through resilience and deterrence	Preparedness Building up the means to face future attack	Readiness Capacity to face future attack

Source: EU

TABLE 3

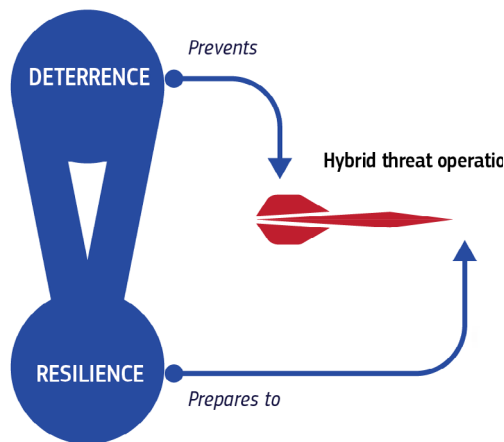
Options to develop deterrence and resilience capacities through practice, simulation and guidance

PRACTICE	Full-scale exercise Live situation to train complete capacities in real-world attack	Joint drill Specialised exercise improving inter-agency or inter-allies cooperation	Manoeuvre Testing deployment and movement of kinetic-oriented capabilities
SIMULATION	Tabletop exercise Scenario-based collective exercise on real world developments	Sandbox Brainstorming to test and optimise situational analysis	Training Capability-based simulation to improve specific competences
GUIDANCE	Workshop Collective examination by domain professionals of specific issues and their teoretical solutions	Seminar Series of meetings to improve knowledge and understanding of domain-related issues	Course Series of lectures aiming at reinforcing knowledge and competences

Source: EU

FIGURE 20

Proactive Anticipation



Source: EU

More on proactive anticipation

- Cumulated at the proactive step, resilience enhances deterrence capacity, while deterrence, in turn, bolsters resilience. Both deterrence and resilience, although firmly situated at the proactive step, remain essential during the active and reactive steps as well.
- Deterrence and resilience are the outcomes of a suite of policies and measures; they must be adapted to each situation to optimise the strategy's overall effectiveness. However, no single solution can address all hybrid threat operations. Adaptability, flexibility and agility are therefore required. Adversaries are aware of criticalities and vulnerabilities; even if they are not, we should assume that they are to avoid strategic surprise.
- Fluid cooperation and coordination mechanisms between institutions at the Member State level are essential: '[s]trong cross government working is a critical enabler in bridging the gap between resilience and wider deterrence' (Roberts, 2019). At the international level, the European security ecosystem constitutes a powerful asset for both deterrence and resilience purposes.
- Proactive anticipation induces the answering of three questions.
 - **Damage factor.** What level of harm is acceptable?
 - **Time factor.** When may it occur?
 - **Spatial factor.** Where would it be inflicted?
- Regarding the impacts and probabilities of hybrid threat operations, vulnerabilities and points of failure (fail-safe / safe to fail) should be analysed. Sharing the resulting information with close allies would strengthen both deterrence and resilience, thereby reinforcing collective security. With close allies would strengthen both deterrence and resilience, thereby, reinforce collective security.

2. ACTIVE DEFENCE

An active defence should be carried out during an attack and immediately afterwards, as swiftly and fluidly as possible. It is organised around three stages (detection–identification–determination (DID)) and two additional elements with specific roles (recovery and attribution).

- **Detection.** Indicators capture signals that an event is occurring.
- **Identification.** Operational-level analysts study the event, its context and its precedents to understand which actor or group of actors is behind it, recognising that it is a hostile operation.
- **Determination.** Strategic-level senior analysts consider the event alongside other ongoing or recent hostile operations using different tools in different domains, highlighting the hybridity of the operation.

The two additional elements are essential and have specific characteristics.

- **Recovery.** Initiated at the detection stage and potentially lasting for a long period, the recovery first ensures business continuity and then restores full capacity.
- **Attribution.** Following the determination stage, attribution is the political statement by decision-makers that officially assigns responsibility to the actor or group of actors behind the hybrid threat operation.

Although these elements do not prescribe a rigid procedure – each European security actor at every level follows its own processes – they outline the essential stages required to actively defend against hybrid threat operations.

2.1. Detection

The first stage of active defence involves analysing data gathered by intelligence services and related agencies (finance, military, infrastructure, etc.)

within a civilian–military framework and converting those data into usable information. This initiates the active defence step and also conditions it, as it relies on high-quality intelligence. Consequently, detection depends heavily on intelligence capabilities, including the ability to identify every tool employed during an operation, a task that is particularly difficult in real time.

Intelligence may originate from governance through specialised entities and also, on a more whole-of-society approach, from the services space and, where appropriate, from the civic space. This three-space approach can enhance intelligence detection and eventually improve EU MS' ability to detect hybrid threat operations. Intelligence originating from the civic or services space can be collected by the governance space and used to enrich its own collection means.

Once centralised in the governance space, intelligence can be shared and analysed through bilateral, minilateral and multilateral formats, for example via the SIAC, linking the European Union Intelligence and Situation Centre (EU INTCEN) and European Union Military Staff (EUMS) Intelligence Directorate. Detection can also be performed by other governance space services, such as health, civil protection, cybersecurity or information security agencies. In the services space, companies can play a critical role in detection, such as being operators of critical infrastructure or cybersecurity companies. In the services space, journalists, open-source intelligence (OSINT) analysts or attentive citizens can prove to be essential in the detection of hybrid threat operations in a whole-of-society approach. Detection therefore implies the ensemble of society and is not strictly limited to intelligence services, although they are central and essential.

Cooperation in detection is essential for several reasons. First, partners may have intelligence on ongoing hybrid activities that the target lacks. Second, allies might be aware of preparatory actions in other tools or domains, enabling deterrence and resilience to be bolstered before an attack is launched. Third, some democratic actors lack

comparable detection capacities, particularly in the maritime, air, space or digital spheres; Member States can share sensors and information bilaterally, minilaterally or multilaterally.

Cooperation is not confined to the governance space. The civic and services spaces also hold powerful assets for detection. Civic actors can contribute, for instance, through social media forensics, first-person-view drones, the uncovering of lawfare, fact checking, investigative journalism or the flagging of unusual conduct. The services sector can provide high-tech inputs across a wide range of fields, from infrastructure and space to cyber, military, intelligence, diplomacy and economics. A systematic strategy that integrates civic and services contributions into detection would offer a decisive advantage in countering hybrid threat operations.

In detection, it is useful to distinguish short-term early-warning indicators from long-term vulnerability indicators. In both cases, however, it would be naive to assume that a completely reliable and exhaustive set of indicators could be devised. The very nature of hybrid threats – particularly within hybrid warfare – means that adversaries continually create innovative actions that outpace any fixed set of indicators.

Consequently, a robust detection system should combine well-known, reliable indicators with an adaptive, on-the-spot detection process that operates as swiftly as possible, extended where necessary to the civic and services spaces' autonomous capabilities (e.g. disinformation, cybersecurity or critical infrastructure). It should also foster the detection of unknown, unusual and unexpected activities, to counter innovative operations. Finally, it should incorporate a technical follow-up to facilitate the detection of new operations weaponising cascading effects. In HIOs involving, for instance, CBRN materials, early detection is essential to contain the immediate and cascading effects and to start the recovery process quickly (7).

Detection should address external hybrid threat actors, but the use of local proxies forms part of a detection–avoidance strategy. As Teija Tiilikainen, Director of Hybrid CoE, explains: '[t]he use of proxies – non-state actors that can interfere in our domestic sphere – helps circumvent existing legis-

lation, allowing them to hide behind other domestic actors, fit more easily into the domestic framework and hinder detection and attribution' (Edwards and Shelat, 2025). This challenging trend calls for the study of recruitment mechanisms and the development of dedicated detection indicators.

2.2. Identification

The second stage of active defence – identification – also relies heavily on intelligence capabilities, but on a more analytical basis. Once the signals related to an attack have been detected, the crucial task is defining which actor or network of actors is behind the operation, as coordinated and parallel attacks have become common. Identification is often the most challenging element of the DID process, because hybrid threat operations are deliberately shrouded in deniability. Recent trends show adversaries employing novel tools and techniques to specifically increase that deniability, avoid identification and, eventually, prevent attribution. Although pinpointing the attacker may sometimes appear impossible, it remains a prerequisite for an effective active defence and efforts should therefore use all possible instruments and contacts to quickly identify the actor behind the operation.

All relevant state services must be incorporated into the identification effort, if needed in a civil–military spirit: first responders, surveillance systems, law enforcement agencies, civil protection bodies, local authorities, medical services, designated focal points and crisis management cells. Cooperation with partners also brings substantial benefits, as allies can provide intelligence on particular tools, methods, operators or strategies, thereby helping to identify the attacker. Cooperation is valuable not only with European partners but also with worldwide allies.

Just as with detection, the civic and services spaces hold information that can markedly improve identification capabilities. While such inputs are sometimes used on a case-by-case basis, a systematic approach would give the services responsible for attribution a decisive advantage. If identification is complicated by the multiplicity of actors, cascading effects can further confound analysts, as one actor may exploit the outcomes of its own operation or one carried out by another.

(7) See, for instance, the Medical Countermeasures Strategy, which refers to a new 'Medifence' initiative (European Commission, 2025d).

In the information domain, for example, countless micro-websites, accounts or channels rebroadcast disinformation that originated elsewhere; tracing responsibility in such a fast-moving environment is certainly difficult.

Nevertheless, identification is only the gateway to subsequent stages of responding effectively. It is therefore of paramount importance that analysts accomplish this stage using innovative instruments and methods where necessary.

2.3. Determination

The third stage, determination, involves transmitting all relevant information about the attack to the strategic level. At this stage, the activities carried out in different domains are considered comprehensively and possibly linked together to decipher the adversary's overall strategy and related ultimate goal.

Even when the actors behind several operations are efficiently identified, grasping the full picture of the aggressor's intentions can be challenging, and the overall situation can remain unclear. The contemporary threat landscape is so intricate that managing all concurrent operations is highly demanding. Tolerable operations can easily be overshadowed by HIOs, yet they may provide low-level signals that help determine the adversary's strategic design. Analysing the saturation of actors and cascading effects, although complex, can provide useful clues.

Applying the comprehensive resilience ecosystem (CORE) model (Jungwirth et al., 2023) provides an effective way of interpreting an operation. The determination analysis should consider the 13 distinct domains across different layers (local, national, international), levels (tactical, operational, strategic) and time scales (short, medium, long). As demonstrated in tabletop exercises and situational analysis, the CORE model offers an analytical framework that makes it possible to highlight the strategy and goal behind a collection of apparently separate operations, even when they involve both state and non-state actors.

The EU Hybrid Fusion Cell (HFC) is ideally placed to analyse multiple operations and provides briefings to the Horizontal Working Party on Enhancing Resilience and Countering Hybrid Threats (HWP ERCHT) on a continuous basis, notably providing valuable contextual information on longer campaigns.

2.4. Recovery

Recovery is intrinsically linked to resilience and also to deterrence by denial, as an adversary will be less likely to attack if society recovers quickly, with limited enduring damage. Nonetheless, recovery can be difficult, particularly regarding specific domains where harm is hard to assess, such as the legal, culture, intelligence and information domains.

A modest level of impact is not necessarily unacceptable. As the concepts of restrictive and cumulative deterrence demonstrate, a defender can tolerate a certain amount of disturbance without jeopardising its business continuity. What matters is that the attack's intensity does not cripple the defender, allowing the targeted domain to recover as quickly as possible and, where possible, be restored to full functionality. When an attack is relatively mild, recovery can be swift and wider society may experience little lasting effect. Even seemingly innocuous actions – such as the limited broadcast of disinformation – can be harmful, as they may erode public trust over the long term or provide a foothold for future actions, with more aggressive operations exploiting the cascading effects. Recovery is therefore an essential task and should be pursued as much as possible, whether the operations are considered individually or collectively.

Recovery offers an important lesson, as it draws on human, material, financial, political and societal resources. Recovery has a price, and the increasing intensity of hybrid threat operations raises that price further. Consequently, resilience through recovery cannot be limitless. The multiple costs associated with recovery therefore provide a strong argument for developing deterrence, because limiting hostile actions can keep those costs within acceptable bounds. In this respect, allowing the aggressor to escape unpunished – even after a swift recovery – risks normalising such conduct and may encourage further operations. Deterrence, including by the imposition of cost, is therefore essential to prevent future attacks.

2.5. Attribution

Hybrid threat operations gain their greatest strength from deniability. By obscuring the true source of an operation, the aggressor can keep the target in a sub-threshold environment and pretend to perceive any response as unjustified and escalatory. This progressive strategic erosion of the

target proceeds until the attacker's objectives are achieved, yet without the attacker incurring heavy – or at least incapacitating – consequences (Kaushal, 2022). As the French president observed, 'the growing hybridity of conflicts (...) blurs all threshold effects' (French Presidency, 2025).

Decision-makers must therefore weigh the costs and benefits of attribution. Because deniability makes identification difficult, attribution typically generates strong reservations, and decision-makers often choose to withhold a public declaration. In the meantime, citizens suffer the consequences of hybrid threat operations without knowing who is responsible for them. Yet attribution is essential for deterrence, as it is generally difficult to respond to hybrid threat operations without attribution, and attribution also underpins resilience. Attribution legitimises policy choices that, if left unattributed, would generate misunderstanding and even potentially disagreement.

Baughman notes that '[a]ccording to a Chinese definition published in the PLA Daily in September 2022, cognitive domain operations "take the human brain as the main combat space, and focus on striking, weakening, and dismantling the enemy's will to fight, using human psychological weaknesses [...] and increasing their internal friction and decision-making doubts"' (McClenon, 2023).

By grounding decisions, attribution makes public actions intelligible to citizens. The German chancellor noted, 'we are not at war, but we are no longer at peace either' (Reuters, 2025b). In this situation that Hoffman (2020) described as 'the messy middle', political leadership and clarity are crucial.

Several Member States have already undertaken initiatives to improve opportunities for attribution, a constructive move for both resilience against and deterrence of hybrid threat operations. Further effort is needed, including a focus on the conditions, actors and processes involved in hybrid threat operations (Jalabert et al., 2025).

Two specific situations can arise, however, where attribution may be ineffective and even potentially counterproductive, namely:

- when low signals underline a probable responsibility in an incoming, current or past attack, without being able to support clear responsibilities (in which case, to cope with this situation, defenders can decide to take actor-agnostic countermeasures without attributing)

- when attribution may potentially imperil a covert reactive response aiming to send a signal to the attacker.

In other cases, when attribution is necessary, a strong attribution is essential. A vague attribution would fail to achieve the intended impact on both the society affected and the adversary. In this respect, two factors should be taken into account.

- **Speed.** A swift attribution enables authorities to implement measures that mitigate the societal impact of the attack and maintain momentum in the response. In some cases, rapid declassification may be required to overcome temporal constraints and allow timely retaliation. In any case, speed is an asset; it enhances the chances of surprising the adversary and of rallying allies.
- **Collectiveness.** An attribution shared by partners reinforces the credibility of the statement and demonstrates strong political engagement. As 'hybrid threats undermine the credibility of deterrence' (Rusinaitė, 2025), collective attribution reinforces the political weight of the declaration and sends a strong strategic signal. As Roberts (2019) explains, 'Adversaries are more likely to fear the imposition of costs if they believe that they will be detected and that the attribution of the attack will be broadly supported.'

Collective attribution, undertaken through any security ecosystem mechanism – whether within the EU framework, by the EU itself or through EU–NATO cooperation – amplifies diplomatic weight and credibility. It signals that the attack is being taken seriously by multiple partners, underscores the close bonds between allies and demonstrates readiness to consider retaliatory measures. Consequently, attribution should, wherever possible, be carried out collectively.

Figures 21 and 22 show the differences between a vague attribution (e.g. lack of content, data and decisiveness) and a strong attribution (e.g. clarity, transparency and leadership). Figure 23 describes the integration of active defence's multiple stages. Example

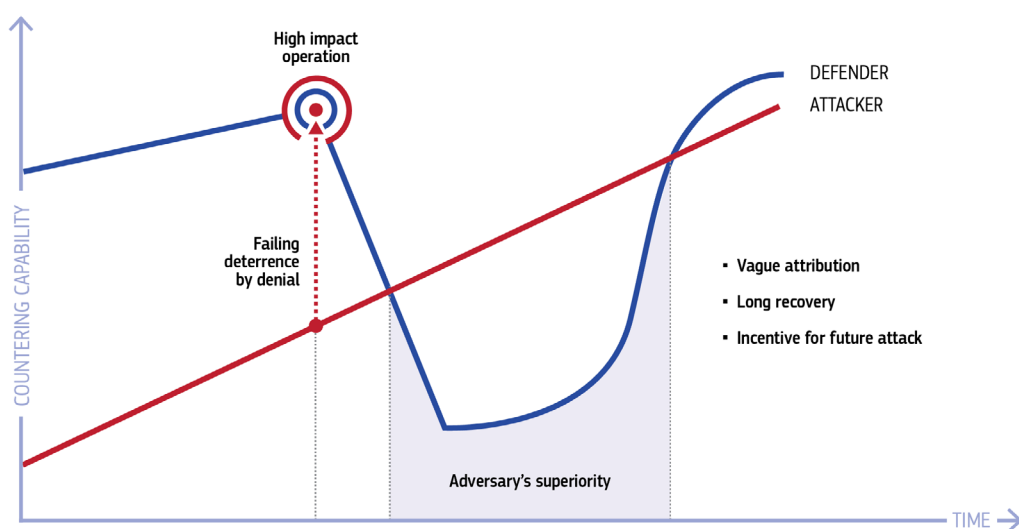
Attribution is decisive in countering hybrid threats. Would an external state wish to undermine the EU's political and military capacity in order to facilitate the invasion of a neighbouring country, its special services could launch a wide-scale attack

leaving a large proportion of citizens in several Member States without electricity. The loss of power would quickly cascade, causing disruptions to communications, water, sewage and emergency services, each of which could be further exploited. The resulting confusion would leave the population demanding an explanation and a remedy. Within hours of the outage, the hostile state could activate a pre-planned disinformation campaign,

claiming that the disturbances are the result of a conspiratorial, malicious plot orchestrated by some of the EU's key allies and selected Member States. In the absence of an official attribution, this narrative would become the first explanation offered to a distressed public, and its deep-seated impact would be difficult to reverse. Two days later, the aggressor could commence a military manoeuvre on the outskirts of the EU's borders, creating a fait

FIGURE 21

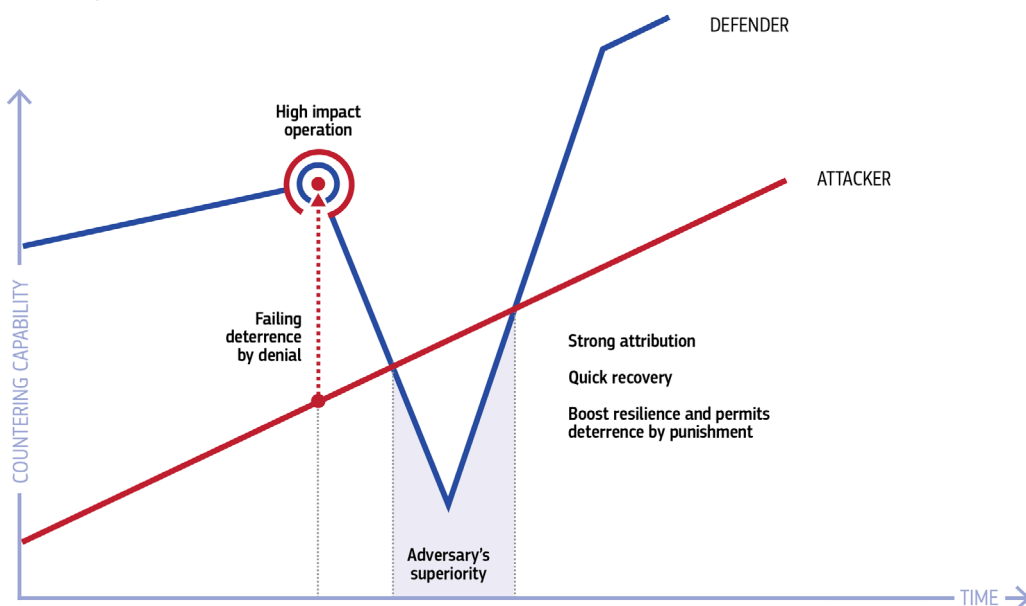
Vague attribution



Source: EU

FIGURE 22

Strong attribution



Source: EU

accompli. Because societies would be inward-looking and demoralised, a coordinated military-political response would become almost impossible.

Even after a period of recovery, European states and their partners would still face political instability. The importance of attribution is therefore evident: if governments cannot definitively explain the cause of the suffering, the civic space remains agitated and confidence in its authorities erodes.

The hostile state's *fait accompli* begins to solidify into a new status quo. Conversely, a strong attribution directs public outrage outward, towards the perpetrator of the HIO. This enables a united coalition response, possibly a retaliatory measure that counters the hostile state's operation. From the standpoint of EU stability, power and economy, this outcome is far preferable.

Attribution and deterrence are thus intrinsically linked. If a hostile state believes that the EU will fail to attribute and therefore will not respond effectively, the operation can proceed with no adverse consequences. This scenario harms the EU in two ways: it must endure the attack and it loses the strategic contest on its periphery, encouraging other hostile actors to follow suit.

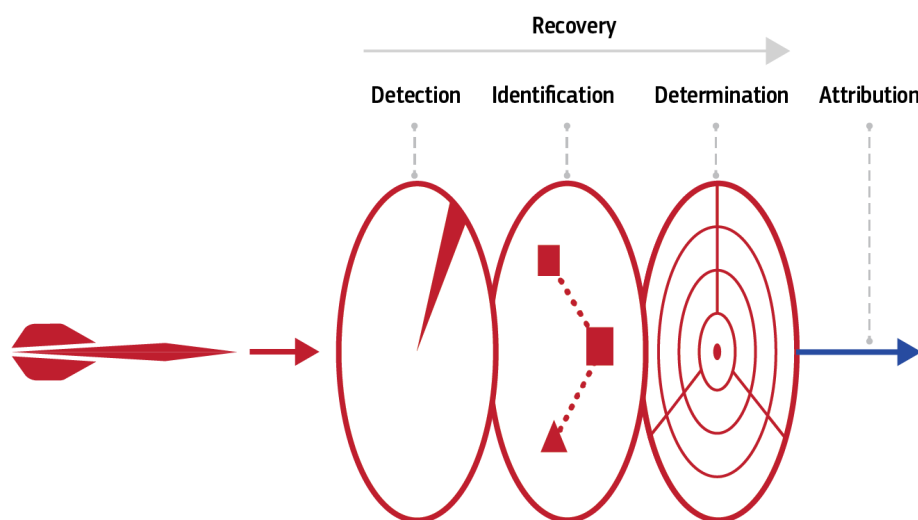
By contrast, if the aggressor assumes that the EU will attribute correctly, it may be deterred. Outrage in European civil society translates into greater unity and stronger countermeasures, reducing the

likelihood of further HIOs – both kinetic and non-kinetic – and limiting the exploitation of cascading effects. In such circumstances, it is safer for EU decision-makers to attribute than to remain silent. Recent developments in the European security ecosystem reveal numerous incidents where no attribution has occurred. The exploitation of cascading effects, often through misinformation that deceives or disorients the public, has significantly shaped public opinion. By retaining the initiative, the hostile actor can weaponise the consequences of its own attack through cascading effects.

The absence of attribution erodes resilience. For example, when media reports portray damage to critical infrastructure in the Baltic Sea as an accident, that might suggest there is no justification for NATO to launch a protective operation such as Baltic Sentry. This creates an opening for hostile actors to present the response as unilateral and hostile, thereby justifying further escalation.

Criminal proceedings can ultimately establish guilt, but they must respect the presumption of innocence and typically take months or years, far too long for the rapid dynamics of hybrid threat operations, where timely attribution is crucial. A parallel investigative track, based on credible intelligence from Member States and allies, should operate autonomously from criminal proceedings, test hybrid threat hypotheses swiftly and support attribution by decision-makers.

FIGURE 23
Active Defence



Source: EU

More on active defence

- The DID process should integrate the three spaces: civic, governance and services. This would improve information quality and increase the likelihood that decision-makers can ultimately attribute responsibility. Such a virtuous circle would strengthen society's resilience to hybrid threat operations.
- The technical-political team responsible for determination must be knowledgeable about all domains affected and the behavioural patterns of the hybrid threat actor. It should also be flexible enough to envision innovative tools or methods being used by the adversary.
- Fluid inter-agency cooperation is essential for a robust defence against hybrid threat operations. The interest of society should be considered the key focus over quarrels.
- Cooperation mechanisms enable extensive exchanges of intelligence, information, actor-related knowledge, contextual understanding, methodological insights, third-party communication channels and best practices. Collective action provides a powerful reinforcement supporting detection, identification, determination, recovery as well as attribution.
- Active defence reinforces deterrence and resilience, operating together at every step.
- Active defence should also consider the long-term impact of hybrid threat operations, recognising the 'synergistic effect' of their 'multi-modal activities' (Hoffman, 2007, p. 8). Beyond their immediate impact, these activities aim to undermine democratic societies collectively over the longer term, through psychosocial and cognitive effects that are difficult to measure.
- Active defence sends an initial message to the aggressor and can be used to test its reaction in preparation for further reactive responses.

3. REACTIVE RESPONSE

The Niinistö report calls for ‘dissuading potential perpetrators through a decisive response that imposes costs outweighing any potential benefits of continued hybrid threat operations’ (Niinistö, 2024, p. 23). To prevent an escalation in intensity and to avoid a slide into more severe conflicts, a response strategy should amplify the adversary’s costs through deterrence. Europe must therefore act swiftly to increase cost imposition within the grey zone by deploying countermeasures.

The distinction between active defence and reactive response is a matter of timing. Active defence takes place during an attack, where emergency measures must be taken rapidly to contain cascading effects and prevent collapse and anarchy. Reactive response follows the attack and constitutes a measured, proportionate response that must be more impactful than the original aggression in order to achieve a deterrent effect.

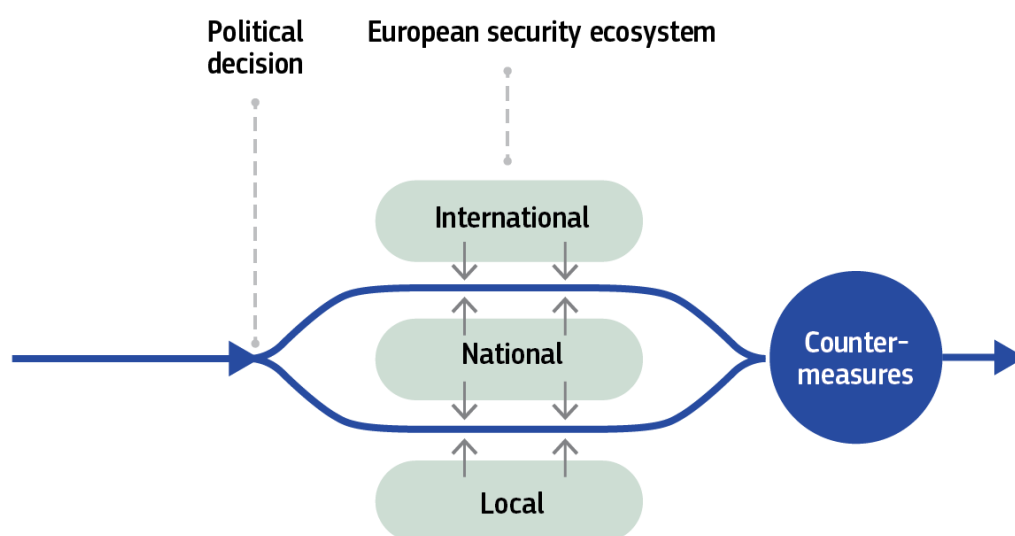
In addition to the implementation of measures in the context of the hybrid toolbox, when further escalation by adversaries becomes evident, collective response can be taken in the EU through the Foreign Affairs Council (FAC) on the recommendation of the Political and Security Committee (PSC), or by the activation of the Integrated Political Crisis Response (IPCR), particularly in the case of HIOs, with the support of intelligence provided by the Hybrid Fusion Cell.

Although it is not currently part of their role, the EU Hybrid Rapid Response Teams (HRRT) could develop to coordinate the resilience and deterrence collective response between EU MS.

Here too, the governance space should work closely with the civic and services spaces, through either established institutional contacts or ad hoc cooperation. Collaboration with other states – whether

FIGURE 24

Reactive Response



Source: EU

they have been directly attacked or not – should be pursued within structured or ad hoc coalitions to reinforce the deterrent effect and to leverage the EU's global power.

It is essential to exploit the particular vulnerabilities of hostile actors in any active countering strategy. As Roberts (2019) observed, 'Deterrence exists in the mind of the adversary, so we not only need to be strong in these areas, we also need to communicate our strengths effectively, whether overtly or covertly, publicly or privately.'

All measures should build on the strengths of democracies and the fragilities of autocracies, employing both negative incentives (retaliation) and positive incentives (opportunities).

The countermeasures proposed in Annex 2 could complement the EU hybrid toolbox, the framework established in 2022 mobilising EU tools for a coordinated EU response to hybrid campaigns, in targeting the specific vulnerabilities of adversarial autocracies. A non-exhaustive but comprehensive list of countermeasures is provided in Annex 2.

Rather than covering all measures, it outlines the instruments that could be used in a democratic framework and shows examples of what responses can be taken to hybrid threat operations. In short, a reactive response constitutes deterrence by punishment against hybrid threat operations (see Figure 24). It is particularly necessary to deter hostile actors from continuing their escalation of hostile actions against European democracies.

More on reactive response

- *The reactive response stage serves a purely defensive purpose and is undertaken only in response to hybrid threat operations.*
- *A reactive response can be carried out only after the attack has been formally attributed by the decision-makers on the basis of a fast-track informational channel based on intelligence services, their cooperation with their peers, as well as the services and civic spaces.*
- *The focus of retaliation should be on horizontal escalation rather than vertical escalation, thereby opening the field to a wide range of democratic tools.*
- *Wherever possible, retaliation should be implemented by the European security ecosystem's various cooperation mechanisms to amplify deterrent effect.*
- *Deception, surprise and disruption must be employed extensively to diminish the aggressor's capacity to anticipate, adapt and strike again.*
- *Retaliation should deliver a strong effect that dissuade the adversary's to rebound, while also achieving a significant strategic impact on other state and non-state adversaries.*

4. RESILIENCE-DETERRENCE STRATEGY

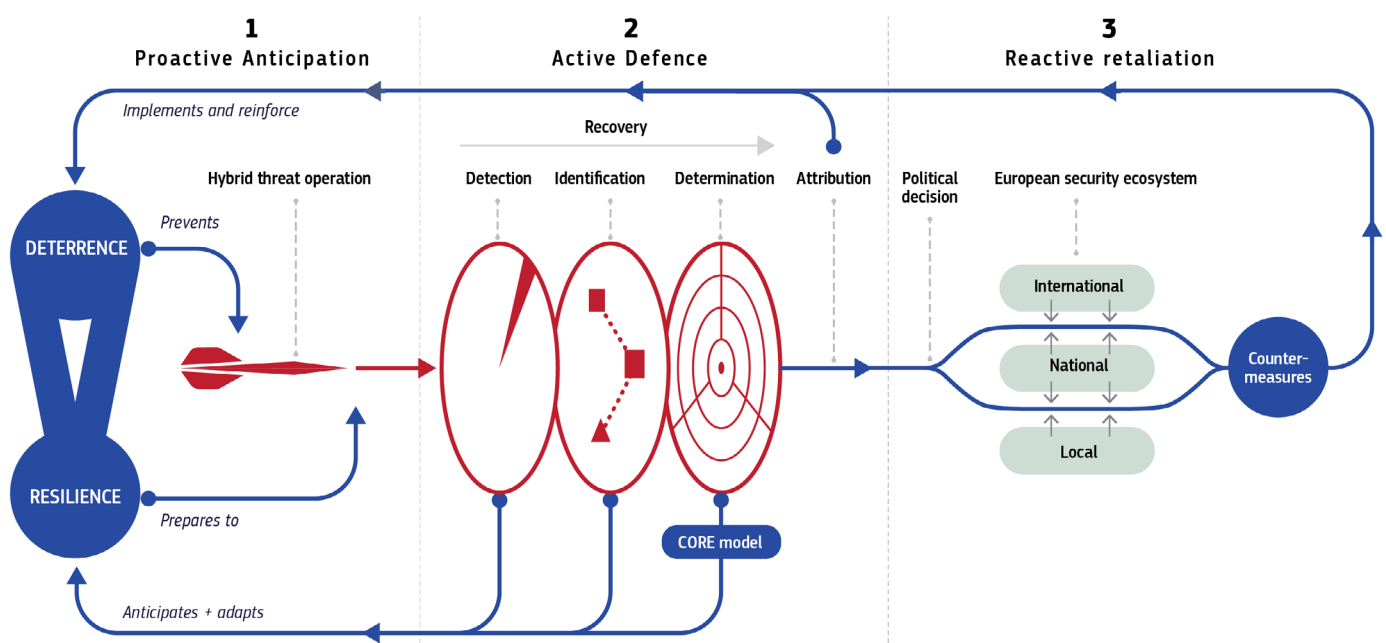
4.1 Shifting the adversary's calculus

The aim of the resilience–deterrence strategy, or RD strategy, is to shift the adversary's calculus by delivering multiple effects.

- Reduced deniability. As the likelihood of successful attribution increases, the adversary is likely to become more cautious about triggering hostile operations in the future.
- Capability depreciation. The combined pressure of resilience and deterrence compels the adversary to reassess its capabilities and the resources it allocates.
- Internal institutional pressure. Repeated failures generate pressure on the adversary's staff, prompting a shift towards softer targets, which should themselves be covered by collective security.
- Ally coherence revelation. An enhanced counterstrategy reshapes the adversary's perception of the coalition, underscoring a stronger resolve and more robust commitment to democracy than was previously anticipated.
- Compressed time horizon. Long-term operations become less attractive when they are reduced to a negligible effect or incur prohibitive costs.
- Reputational accumulation. Repeated attributions and the visible imposition of costs cause reputational damage to the adversary.

FIGURE 25

Reactive Response



Source: EU

4.2 The strategy

The RD strategy is intended to operate as a self-reinforcing loop, with several returns that consolidate resilience and deterrence at every one of its three steps (Figure 25).

- 1. Proactive anticipation** seeks to dissuade future hybrid threat operations while still preparing for the possibility that they may occur. In this step, resilience and deterrence converge, because resilience creates the denial capability that underpins deterrence.
- 2. Active defence** strengthens addresses on-going hybrid threat operations and enables attribution. By reinforcing the strategy through the loop, active defence refines resilience, allowing future operations to be anticipated more effectively, while simultaneously degrad-

ing the adversary’s expected return. Successful attribution reinforces deterrence against subsequent attacks.

- 3. Reactive response** imposes costs on the aggressor through countermeasures, thereby discouraging further hostile actions. By reinforcing the strategy through the loop, this component markedly bolsters deterrence, altering the adversary’s cost–benefit calculus. In addition, as deterrence becomes stronger, the burden on resilience diminishes.

4.3. Risks

As shown in Table 4, several issues can reduce the efficiency of the RD strategy, but they can be mitigated.

TABLE 4
Risks

RISK	MITIGATION
Siloed resilience investment	Resilience should be pursued via a comprehensive approach that integrates all thirteen domains, rather than being confined to isolated sectors.
Deterrence crowding out resilience	While deterrence is essential, it must not dominate the agenda to the detriment of resilience; a measured pace is required to avoid creating gaps that adversaries could exploit.
Attribution bandwidth consumed by crisis	To prevent delays that might trigger cascading effects, decision-makers must carry out attribution promptly, using the intelligence available and underpinned by firm political resolve.
Alliance arbitrage	Solidarity mechanisms alone are insufficient; resilience and deterrence must be coordinated collectively to stop adversaries from targeting weaker partners and attempting to divide the coalition.
Baseline erosion	To halt the gradual erosion of societies by saturation, high impact operations and cascading effects, efforts must be coherent and sustained, encompassing both short term actions and long term strategies.
Strategy too successful	To guard against the risk of political disinvestment if the counter-strategy proves excessively effective, a long-term framework with adaptive measures should be established.

Source: EU

5. CASE STUDIES

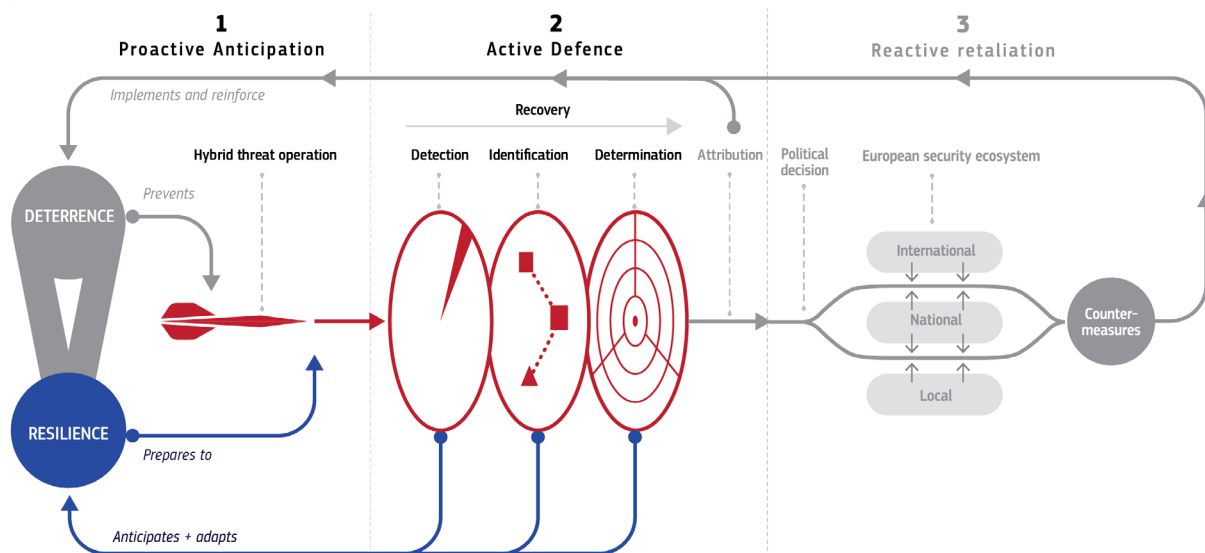
5.1 Case study 1: resilience only

When resilience constitutes the exclusive strategic paradigm, the mitigation of hybrid threat operations regresses to a reactive posture, perpetually lagging behind the requisite efforts to deter assaults. The defender becomes ensnared in a perpetual cycle of adaptation, diverting escalating resources towards resilience. From the adversary's vantage point, this relentless commitment to defensive posture is seen as a provocative stimulus, inciting an intensification of attacks until the defender's capacity for resistance is ultimately subsumed.

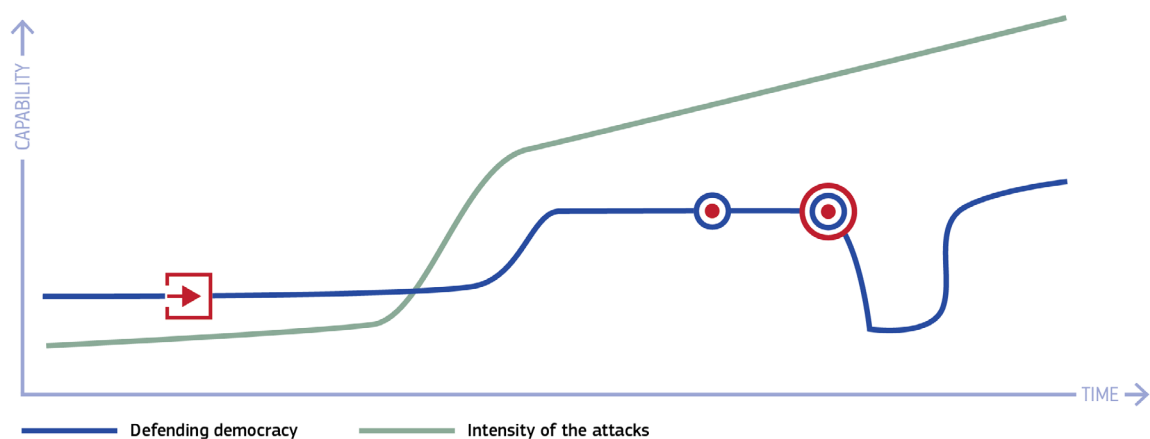
FIGURE 26

Case study 1: Resilience only

RD STRATEGY



IMPACT



Source: EU

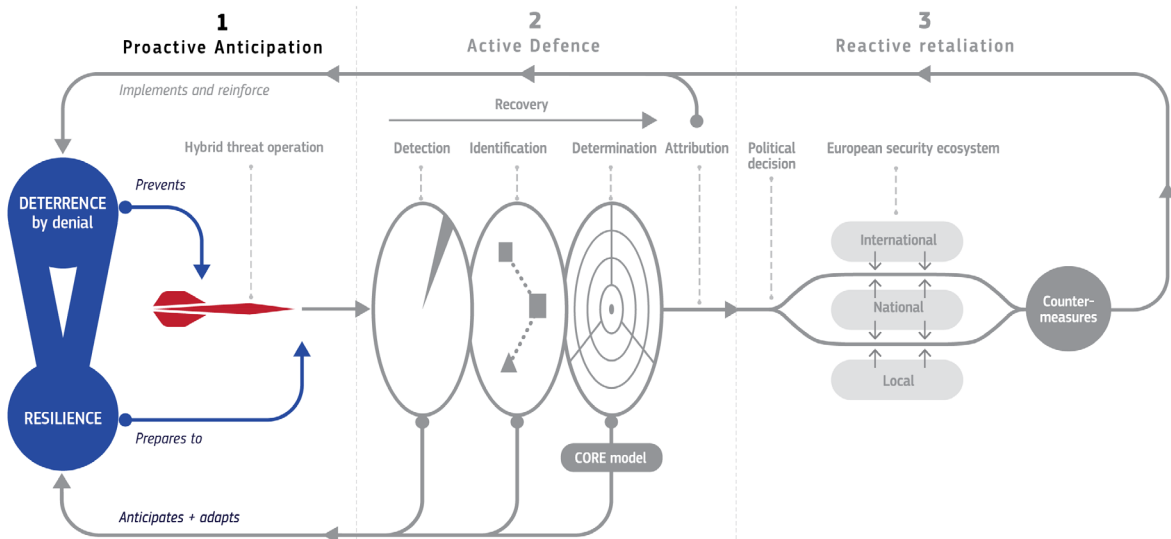
5.2 Case study 2: deterrence by denial

Resilience is integrated with deterrence by denial, culminating in a robust and successful mitigation strategy designed to preclude hybrid threat operations. The adversary's malevolent incursions are effectively neutralised, thereby circumventing the infliction of substantial harm upon the defending democracy. This approach base entirely on proactive anticipation engenders a judicious conservation of resources preserving efforts for resilience.

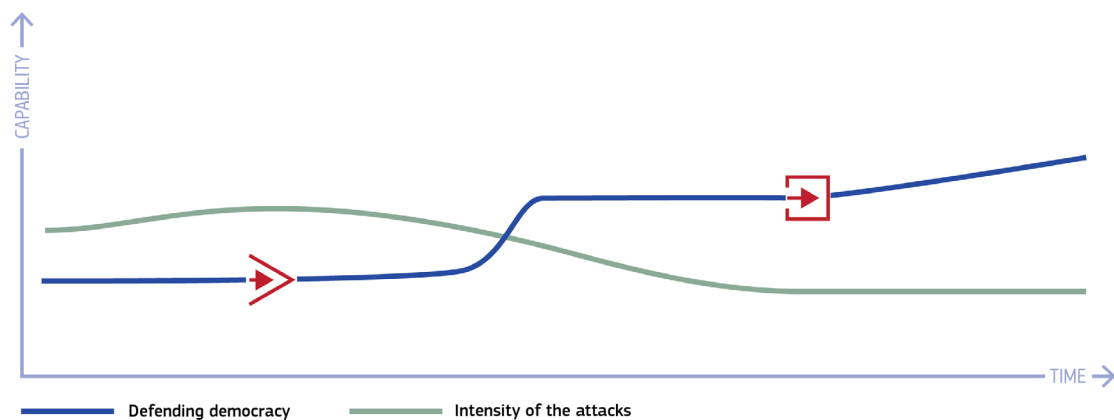
FIGURE 27

Case study 2: Resilience and deterrence by denial

RD STRATEGY



IMPACT

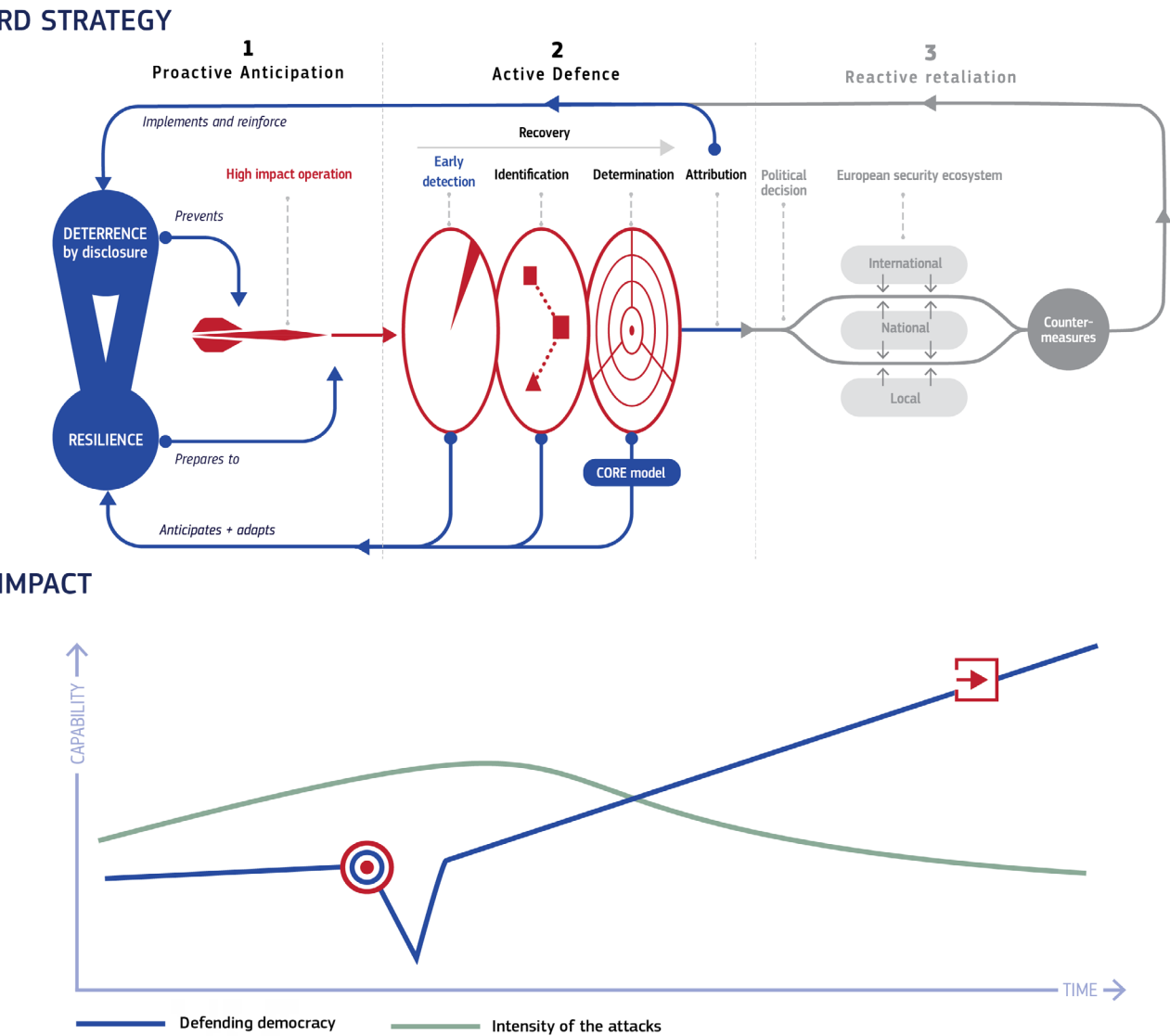


Source: EU

5.3 Case study 3: early detection and deterrence by disclosure against a high impact operation

Resilience is here strategically combined with deterrence by disclosure, facilitated by the timely detection of a high impact operation. Upon attribution, the efficacy of the adversarial attack is significantly curtailed, owing to the defending democracy's proactive capacity to fortify its resilience measures in anticipation of such incursions. The resultant impact manifests in the form of expedited recovery and a diminution in the intensity of subsequent adversarial operations.

FIGURE 28
Case study 3: Resilience and deterrence by punishment against a high-impact operation



Source: EU

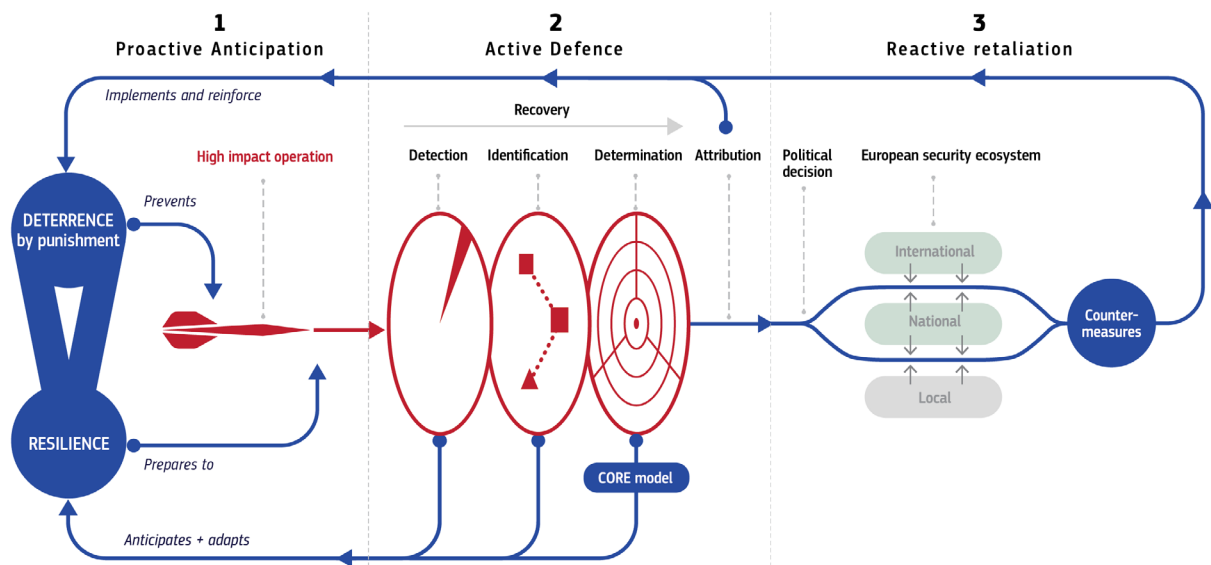
5.4 Case study 4: deterrence by punishment against a high impact operation

In this instance, resilience is associated with deterrence by punishment. Confronted with a high impact operation, the defending democracy attributed the attack and undertook the political decision to enact step 3, reactive response, at national and international layers. A multifaceted combination of countermeasures is subsequently executed, whilst the defender enhances its capability after a swift recovery. This approach exerts a tangible impact upon the adversary, concomitantly attenuating the intensity of future hostile operations.

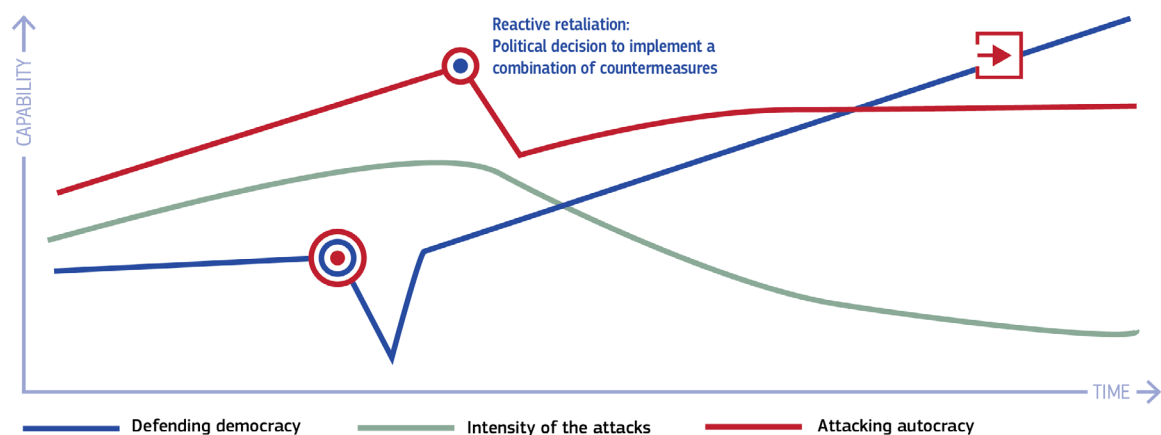
FIGURE 29

Resilience and deterrence by disclosure with early detection against a high-impact operation

RD STRATEGY



IMPACT



Source: EU

6. CONCLUSIONS

The international security landscape is rapidly evolving, with Europe facing an existential challenge posed by escalating hybrid threat operations. These threats, though maintained under the threshold of formally declared war, endanger European security, democracy, and solidarity.

At the operational level, this transformation is characterised by a saturation of operations, the weaponisation of cascading effects, and the execution of high impact operations. Collectively, these trends attempt to drive EU member states into inextricable situations aiming at their destabilisation.

Strategically, hybrid threat operations have intensified across multiple domains, and their array of tools has aggravated. The situation has escalated to hybrid warfare, representing the “hard end” of the hybrid threat spectrum. This evolution necessitates a strong adaptation in Europe's countering response.

To this end, the report's proposal of a resilience-deterrence (RD) strategy works as a self-reinforcing loop, integrating proactive anticipation, active defence, and reactive response.

Proactive anticipation combines resilience and deterrence to dissuade future hybrid threat operations while preparing contingency measures. Active defence focuses on the operational phase (detection, identification, determination), while implementing recovery and, as much as possible, attribution. Permitted by this last step, political decision triggers reactive response to amplify the adversary's costs through countermeasures.

The overarching objective of the RD strategy is to alter the adversary's calculus by reducing deniability, depreciating adversarial capabilities, mitigating internal institutional pressure, enforcing ally solidarity, and preventing the adversary's hostile operations in the long-term.

In summary, this report aims to scientifically expose Europe's new threat landscape and propose a strategic model and operational instruments to better contain escalation by deterring both state and non-state adversaries. European democracies are being challenged, but they can prevail, together.

REFERENCES

- Adamsky, D. (2023a), 'Genealogy of deterrence à la Russe', In: Adamsky, D., The Russian Way of Deterrence, Stanford University Press, 2023. <https://www.sup.org/books/politics/russian-way-deterrence>.
- Adamsky, D. (2023b), 'Strategic culture and deterrence scholarship', In: Adamsky, D., The Russian Way of Deterrence, Stanford University Press, 2023. <https://www.sup.org/books/politics/russian-way-deterrence>
- AFP/Euractiv, 'Germany to harden critical infrastructure as Russia fears spike', Euractiv, 29 January 2026. www.euractiv.com/news/germany-to-harden-critical-infrastructure-as-russia-fears-spike/
- Albertini, A., 'Le patron de la gendarmerie met en garde ses troupes contre « la possibilité d'un conflit armé »', Le Monde, 27 January 2025. http://www.lemonde.fr/societe/article/2025/01/27/le-patron-de-la-gendarmerie-met-en-garde-ses-troupes-contre-la-possibilite-d-un-conflit-arme_6519196_3224.html
- Allison, G., 'Intelligence warns Russia 'preparing for war with NATO'', UK Defence Journal, 17 February 2025. <https://ukdefencejournal.org.uk/intelligence-warns-russia-preparing-for-war-with-nato/>
- Atkins, W., 'Defense Policy Resilience in the Face of Black Swans and Grey Rhinos', In: Krieger, M., Chandler Garcia, L. M., Riley, J. H. & Atkins, W. (Eds.), American Defense Policy, Ninth Edition, Johns Hopkins University Press, 2021. <https://books.google.be/books?id=b646EAAAQBAJ&printsec=frontcover&hl=nl#v=onepage&q&f=false>
- Audinet, M. & Gérard, C., 'Under the radar - Crisis, reorganization and clandestinization in Russia's ecosystem of information influence after the invasion of Ukraine', Réseaux, Vol.3, No. 245, 2024, pp.113-152. <https://shs.cairn.info/revue-reseaux-2024-3-page-113>
- Austin, L. J., 'Secretary of Defense Austin Remarks at the Global Emerging Technology Summit of The National Security Commission on Artificial Intelligence (As Delivered)', Transcript, U.S. department of war, 13 July 2021. <https://www.war.gov/News/News-Stories/Article/Article/2592149/defense-secretary-says-integrated-deterrence-is-cornerstone-of-us-defense/>
- Bach Nyemann, D. & Sørensen, H., 'Going Beyond Resilience. A revitalised approach to countering hybrid threats', Hybrid CoE Strategic Analysis 13, European Centre of Excellence for Countering Hybrid Treats (Hybrid CoE), November 2018. www.hybridcoe.fi/wp-content/uploads/2020/07/Strategic-analysis-13-Sorensen-Nyeman.pdf
- Baisotti, P., 'China's Charm Offensive in Latin America and the Caribbean: A Comprehensive Analysis of China's Strategic Communication Strategy Across the Region [Part II: Influencing the Media]', Research Publications 56, Florida International University, 2023. https://digitalcommons.fiu.edu/jgi_research/56
- Baltic Assembly, 'Baltic parliamentarians address security cooperation of the Baltic States and challenges in the region', 15 May 2023. www.baltasam.org/baltic-parliamentarians-discuss-security-Riga
- Barbu, M., Lukiv, J. & Graham, C., 'Nato and EU condemn Russia after drone hits Romanian residential block', BBC, 29 May 2026. www.bbc.com/news/articles/c93x4nxlkjeo
- Batista Cabanas, L. & Heinz, E., 'Mass drone warfare is Europe's rising security threat', Euronews, 14 April 2026. www.euronews.com/my-europe/2026/04/14/mass-drone-warfare-is-europes-rising-security-threat
- Baumann, M. & Pynnöniemi, K., 'European Security in the Era of Hybrid Warfare', DGAP Policy Brief, Deutsche Gesellschaft für Auswärtige Politik (DGAP), 05 November 2025. <https://dgap.org/en/research/publications/european-security-era-hybrid-warfare>

- Bayer, L. and Trevelyan, M. 'Russia sends nuclear warning to NATO as tensions rise in the Baltic', Reuters, 30 September 2026. www.reuters.com/business/aerospace-defense/russia-issues-nuclear-warning-nato-tensions-rise-baltic-2026-09-30/
- Beznosiuk, M., 'Putin's hybrid war against Europe continues to escalate', UkraineAlert, Atlantic Council, 25 August 2025. www.atlanticcouncil.org/blogs/ukrainealert/putins-hybrid-war-against-europe-continues-to-escalate/
- Bicchieri, C., 'Rationality and Game Theory', In: Mele, A. R. & Rawling, P. (Eds.), The Oxford Handbook of Rationality, pp. 182–205, 02 September 2009. <https://doi.org/10.1093/oxfordhb/9780195145397.003.0010>
- Brady, A.-M., 'When China knocks at the door of New Caledonia', Australian Strategic Policy Institute (ASPI), 23 August 2024. www.aspi.org.au/report/when-china-knocks-door-new-caledonia/
- Brands, H. & Cooper, Z., 'Dilemmas of Deterrence: The United States' Smart New Strategy Has Six Daunting Trade-offs', The Marshall Papers, Center for Strategic and International Studies, 12 March 2024. www.csis.org/analysis/dilemmas-deterrence-united-states-smart-new-strategy-has-six-daunting-trade-offs
- Braw, E., 'How to Involve Civil Society in Grey Zone Defence', in Regan, M. & Sari, A. (eds), Hybrid Threats and Grey Zone Conflict: The Challenge to Liberal Democracies, Ethics, National Security, and the Rule of Law, Oxford University Press, 2024. <https://doi.org/10.1093/oso/9780197744772.003.0025>
- Burkhard, T., 'Strategic Vision of the Chief of Defense Staff', French Staff of the Armed Forces, Ministry of the Armed Forces, October 2021, www.defense.gouv.fr/sites/default/files/ema/211022_EMACOM_Strategic-Vision_UK_Vdef_HQ%20%283%29.pdf
- Burrows, E., 'Intelligence officials worry a sabotage campaign blamed on Russia is growing more dangerous', The Associated Press, 10 July 2025. <https://apnews.com/article/russia-sabotage-europe-ukraine-13ee37cf869139839f0d4a3ebe7bd80d>
- Campbell, A. & Armstrong, K., 'Three men found guilty of Wagner-linked arson attack in London', BBC, 08 July 2025, www.bbc.com/news/articles/cx2k37x91vlo
- Chancellery of the Prime Minister of the Republic of Poland, 'PM Tusk: Poland Must Seal Entire Border with Russia and Belarus', 20 May 2025. www.gov.pl/web/primeminister/pm-tusk-poland-must-seal-entire-border-with-russia-and-belarus
- Charter of Trust, 'Hybrid Threats – An Expert's Playbook on Cybersecurity', 14 February 2025. https://securityconference.org/assets/01_Bilder_Inhalte/05_Marketplace_of_Ideas/Charter_of_Trust_Hybrid_Threats_Report.pdf
- Cohen, E. A., 'Who Perseveres, Wins', The Atlantic, Ideas, 24 May 2024. www.theatlantic.com/ideas/archive/2022/05/stakes-of-ukraine-winning-russia-war/631642/
- Council of the European Union, 'Hybrid threats/Russia: Statement by the High Representative on behalf of the EU on Russia's continued hybrid activity against the EU and its Member States', Press release 8 October 2024. www.consilium.europa.eu/en/press/press-releases/2024/10/08/hybrid-threatsrussia-statement-by-the-high-representative-on-behalf-of-the-eu-on-russia-s-continued-hybrid-activity-against-the-eu-and-its-member-states/
- Council of the European Union, 'Hybrid threats / Russia: Statement by the High Representative on behalf of the EU condemning Russia's persistent hybrid campaigns against the EU, its Member States and partners', Statements and remarks, 18 July 2025. www.consilium.europa.eu/en/press/press-releases/2025/07/18/hybrid-threats-russia-statement-by-the-high-representative-on-behalf-of-the-eu-condemning-russia-s-persistent-hybrid-campaigns-against-the-eu-its-member-states-and-partners/
- Council of the European Union, 'Council conclusions on advancing the European Union's capacity to counter hybrid threats', 7349/26, 16 March 2026. <https://data.consilium.europa.eu/doc/document/ST-7349-2026-INIT/en/pdf>

- D'Cunha, S., Ferraro, T. & Rodenhäuser, T., 'Hybrid threats', 'grey zones', 'competition', and 'proxies': When is it actually war?, Humanitarian Law and Policy, International Committee of the Red Cross (ICRC), 16 January 2025. <https://blogs.icrc.org/law-and-policy/2025/01/16/hybrid-threats-grey-zones-competition-and-proxies-when-is-it-actually-war/>
- Darnley-Stuart, A. & Edwards, D. (Hosts), 'SOF and Influence Activities' [Audio podcast episode], No. 116, Irregular Warfare Podcast, Irregular Warfare Initiative (IWI), 17 October 2024. <https://irregularwarfare.org/podcasts/sof-in-competition-special-project/>
- Dobbinga, B., 'Research: Europe increasingly targeted by Russian sabotage', Universiteit Leiden, 20 January 2025. www.universiteitleiden.nl/en/news/2025/01/research-europe-increasingly-targeted-by-russian-sabotage
- Ducaru, S., Nițu, I. & Margvelashvili, M. (Eds.), Black Swan Events on NATO's Eastern Flank, NATO Science for Peace and Security Studies, E: Human and Societal Dynamics, Vol. 143, IOS Press in cooperation with NATO Emerging Security Challenges Division, 2019. <https://ebooks.iospress.nl/volume/black-swan-events-on-natos-eastern-flank>
- Dunlap, C. J. D., 'Guest Post: Dr. Frank Hoffman on "Conceptualizing Integrated Deterrence"', Lawfire, 8 January 2022. <https://sites.duke.edu/lawfire/2022/01/08/guest-post-dr-frank-hoffman-on-conceptualizing-integrated-deterrence/>
- Dunlop, T., 'Germany warns Russia may be preparing attack on NATO', UK Defence Journal, 29 March 2025. <https://ukdefencejournal.org.uk/germany-warns-russia-may-be-preparing-attack-on-nato/>
- Dutch National Coordinator for Counterterrorism and Security, 'Prepare for an emergency situation', 25 November 2025. <https://english.denkvooruit.nl/information-booklet2025>
- Dylan, H. & Maguire, T. J., 'Secret Intelligence and Public Diplomacy in the Ukraine War', Survival, Vol. 64, No. 4, pp. 33–74, 2022. <https://doi.org/10.1080/00396338.2022.2103257>
- Dyner, A. M., 'Russia Continuing Cyberthreats Against NATO Countries', The Polish Institute of International Affairs (PRISM), 21 November 2023. <https://pism.pl/publications/russia-continuing-cyberthreats-against-nato-countries>
- Edelman, E. S., 'The Pros and Cons of 'Deterrence by Disclosure'', The Dispatch, 21 February 2022. https://thedispatch.com/article/the-pros-and-cons-of-deterrence-by/?utm_source=url
- Edwards, C. & Seidenstein, N., 'The Scale of Russian Sabotage Operations Against Europe's Critical Infrastructure', The International Institute for Strategic Studies (IISS), 19 August 2025. www.iiiss.org/research-paper/2025/08/the-scale-of-russian-sabotage-operations-against-europes-critical-infrastructure/
- Edwards, D. & Shelat, N. (Hosts), 'Plausible Deniability: Proxy Actors and the Hybrid Threat Ecosystem' [Audio podcast episode], No. 126, Irregular Warfare Podcast, Irregular Warfare Initiative (IWI), 04 April 2025. <https://irregularwarfare.org/podcasts/sof-in-competition-special-project/>
- European Broadcasting Union (2025a), Investigative Journalism Network, 'Playing With Fire Are Russia's hybrid attacks the new European war?', 12 March 2025. <https://investigations.news-exchange.ebu.ch/playing-with-fire-are-russias-hybrid-attacks-the-new-european-war/>
- European Broadcasting Union (2025b), 'EBU contribution to the European Commission consultation on the European Democracy Shield', 27 May 2025. www.ebu.ch/files/live/sites/ebu/files/News/Position_Papers/open/2025/EBU_DemocracyShield_public%20consultation.pdf
- European Commission (2020a), '2020 Strategic Foresight Report, Charting the Course Towards a More Resilient Europe', 9 September 2020. https://commission.europa.eu/document/download/497a17be-3824-4135-bf2b-1072d74272b3_en?filename=strategic_foresight_report_2020_1.pdf
- European Commission (2020b), 'European Democracy Action Plan: making EU democracies stronger', 03 December 2020, https://ec.europa.eu/commission/presscorner/detail/ga/ip_20_2250

European Commission, 'Tackling R&I foreign interference', Staff working document, Publications Office of the European Union, 2022, <https://data.europa.eu/doi/10.2777/513746>

European Commission, 'Commission steps up support for Member States to strengthen EU security and counter the weaponisation of migration', 11 December 2024. https://ec.europa.eu/commission/presscorner/detail/en/ip_24_6251

European Commission (2025a), 'Speech by President von der Leyen at the European Parliament plenary debate on a united response to recent Russian violations of the EU Member States' airspace and critical infrastructure', Speech08 October 2025. https://ec.europa.eu/commission/presscorner/detail/en/speech_25_2316

European Commission (2025b), 'White Paper for European Defence – Readiness 2030', 19 March 2025. https://commission.europa.eu/document/download/e6d5db69-e0ab-4bec-9dc0-3867b4373019_en?filename=White%20paper%20for%20European%20defence%20-%20Readiness%202030.pdf

European Commission (2025c), 'Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on ProtectEU: a European Internal Security Strategy', COM(2025) 148 final, 01 April 2025. <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52025DC0148>

European Commission (2025d), Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Preparing the EU for the next health crisis: a Medical Countermeasures Strategy, COM(2025) 529 final. https://health.ec.europa.eu/document/download/1be3e462-bd50-4c64-b147-add9d1d5a580_en?filename=com_2025-529-1_act_en.pdf

European Commission (2025e), '2025 Rule of law report - Communication and country chapters', 8 July 2025, https://commission.europa.eu/publications/2025-rule-law-report-communication-and-country-chapters_en

European Commission (2025f) The Code of Conduct on Disinformation, 13 February 2025. <https://digital-strategy.ec.europa.eu/en/library/code-conduct-disinformation>

European Commission (2026a), 'EU Civil Protection Mechanism'. https://civil-protection-humanitarian-aid.ec.europa.eu/what/civil-protection/eu-civil-protection-mechanism_en

European Commission (2026b), Speech by Commissioner Kubilius at the Folk och Försvar – National Conference 2026: "Europe Under Pressure", 11th January 2026. https://ec.europa.eu/commission/presscorner/detail/en/speech_26_69

European Commission, 'Resilience reports', The Joint Research Centre: EU Science Hub, no date. https://joint-research-centre.ec.europa.eu/projects-and-activities/resilience/resilience-reports_en

European Commission & High Representative of the Union for Foreign Affairs and Security Policy, 'Joint Communication to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions on the European Preparedness Union Strategy', JOIN(2025) 130 final, 26 March 2025. <https://webgate.ec.europa.eu/circabc-ewpp/d/d/workspace/SpacesStore/b81316ab-a513-49a1-b520-b6a6e0de6986/file.bin>

European External Action Service, 'A Strategic Compass for Security and Defence – For a European Union that protects its citizens, values and interests and contributes to international peace and security', 21 March 2022. https://www.eeas.europa.eu/sites/default/files/documents/strategic_compass_en3_web.pdf

European External Action Service (2025a), 'Defence: Speech by High Representative/Vice-President Kaja Kallas at the Annual Conference of the European Defence Agency', 01 January 2025. www.eeas.europa.eu/eeas/defence-speech-high-representativevice-president-kaja-kallas-annual-conference-european-defence_en

European External Action Service (2025b), 'European Union Rapid Deployment Capacity', May 2025. www.eeas.europa.eu/sites/default/files/documents/2025/2025-EU-Rapid-Deployment-Capacity_EN.pdf

- European External Action Service (2026a), 'Keynote speech by HRVP Kaja Kallas at the 2026 Conference on Countering Foreign Information Manipulation and Interference: 'From Insight to Impact'', 17 March 2026. www.eeas.europa.eu/eeas/keynote-speech-hrvp-kaja-kallas-2026-conference-countering-foreign-information-manipulation-and-interference
- European External Action Service (2026b), 'Nordic-Baltic Eight: Press remarks by High Representative/Vice President Kaja Kallas at the joint press conference with Foreign Ministers', 30 April 2026. www.eeas.europa.eu/eeas/nordic-baltic-eight%20press%20remarks%20high-representativevice-president-kaja-kallas%20-%20joint%20press
- European Organisation for Security (EOS), Critical Infrastructure Protection – The Need for a European Security Fund, Position paper, June 2024. www.eos-eu.com/Files/Publications/EOS%20position%20on%20the%20need%20of%20an%20ESF%20for%20infrastructure%20protection.pdf
- European Parliament, 'European Parliament resolution of 8 February 2024 on Russiagate: allegations of Russian interference in the democratic processes of the European Union (2024/2548(RSP))', P9_TA(2024)0079, RC-B9-0124/2024, 8 February 2024, www.europarl.europa.eu/doceo/document/TA-9-2024-0079_EN.html
- European Parliament (2025a), 'European Parliament Press Kit for the European Council of 18–19 December 2025', News/Press releases, 18 December 2025. www.europarl.europa.eu/news/en/press-room/20251217IPR32257/european-parliament-press-kit-for-the-european-council-of-18-19-december-2025
- European Parliament (2025b), 'European Democracy Shield In "Protecting our democracy, upholding our values"', Legislative Train Schedule, 15 August 2025. www.europarl.europa.eu/legislative-train/theme-protecting-our-democracy-upholding-our-values/file-european-democracy-shield
- European Parliament, 'Draft Report on hybrid warfare and the protection of the EU's territorial integrity and critical security and defence infrastructure', Committee on Security and Defence (SEDE), (2026/2024(INI)), 08 May 2026. www.europarl.europa.eu/meetdocs/2024_2029/plmrep/COMMITTEES/SEDE/PR/2026/06-03/1343474EN.pdf
- European Parliament and the Council of the European Union, 'Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC (Text with EEA relevance)', PE/51/2022/REV/1 OJ L 333, 27 December 2022, pp. 164–198. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32022L2557>
- European Space Agency (2026a), 'Saturation of Inter Satellite Links', Space Attacks and Countermeasures Engineering Shield (SPACE-SHIELD). <https://spaceshield.esa.int/techniques/T2052/>
- European Space Agency (2026b), Saturation/Exhaustion of Spacecraft Resources, Space Attacks and Countermeasures Engineering Shield (SPACE-SHIELD). <https://spaceshield.esa.int/techniques/T2053/>
- European Strategy and Policy Analysis System (ESPAS), 'About ESPAS', no date. www.espas.eu/about.html
- European Union, 'Making critical entities more resilient', Summaries of EU Legislation, 19 February 2024. <https://eur-lex.europa.eu/EN/legal-content/summary/making-critical-entities-more-resilient.html#:~:text=Resilience,terrorism%2C%20sabotage%20or%20hybrid%20threats>
- Everts, S., 'Resilience alone is not enough in the hybrid war with Russia', European Union Institute for Security Studies (EUISS), 19 February 2025. www.eiss.europa.eu/publications/commentary/resilience-alone-not-enough-hybrid-war-russia
- Finnish Ministry of the Interior, 'Prepared People Cope Better', 2024. https://cdn.verkkopalvelu.suomi.fi/files/varautunut-parjaa-paremmiin_SM_englantti-56a3727e1c9bf6621eb5e57bc4e383bf.pdf
- France 24, 'New drones sighted over Denmark's largest military base', 27 September 2025. www.france24.com/en/europe/20250927-new-drones-sighted-over-denmark-s-largest-military-base
- Freedman, L., Deterrence, Polity Press, 2004.

- Freedman, L., 'Beyond Deterrence And its limits in the Russo-Ukrainian War', Comment is Free, 04 December 2024. <https://samf.substack.com/p/beyond-deterrence>
- French Government, 'Tous responsables', 20 novembre 2025. <http://www.info.gouv.fr/upload/media/mixed/0001/15/c5063e079da84ccc3e422df5f9ca7791d8ab2649.pdf>
- French Presidency, Discours du Président de la République sur l'Europe à la Sorbonne, 25 avril 2024. www.elysee.fr/emmanuel-macron/2024/04/24/discours-sur-leurope
- French Presidency, 'Discours du Président de la République aux armées depuis l'Hôtel de Brienne', 13 juillet 2025. www.elysee.fr/emmanuel-macron/2025/07/13/discours-aux-armees-depuis-lhotel-de-brienne
- Gardner, F., & Wong, T., 'Russia may attack NATO in the next four years, German defence chief warns', BBC News, 01 June 2025. <https://www.bbc.com/news/articles/c62v63gl8rvo>
- Geers, K., 'Strategic Cyber Security', NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), June 2011. https://ccdcOE.org/uploads/2018/10/2011_Proceedings_0-1.pdf
- German Federal Foreign Office, 'Joint Declaration by the Foreign Ministers of Germany, France, Poland, Italy, Spain and the United Kingdom in Warsaw', Press Release, 19 November 2024. www.auswaertiges-amt.de/en/newsroom/news/2685538-2685538
- Giannopoulos, G., Smith, H., Theocharidou, M., 'The Landscape of Hybrid Threats: A conceptual model', EUR 30585 EN, Publications Office of the European Union, Luxembourg, 2021, ISBN 978-92-76-29819-9, https://doi.org/10.2760/44985_JRC123305
- Giles, K., 'Russia's "New" Tools for Confronting the West – Continuity and Innovation in Moscow's Exercise of Power', Russia and Eurasia Programme, Chatham House, March 2016. <https://www.chathamhouse.org/sites/default/files/publications/2016-03-russia-new-tools-giles.pdf>
- Government of the Netherlands, 'Statement of the European Coalition for Civil Preparedness', 22 May 2025. www.rijksoverheid.nl/binaries/rijksoverheid/documenten/publicaties/2025/05/22/joint-statement-european-coalition-on-civil-preparedness-and-resilience/Joint+Statement+European+Coalition+on+Civil+Preparedness+and+Resilience.pdf
- Grare, F., 'Russia, Azerbaijan exploit New Caledonian strife against France; China stays mum', The Strategist, Australian Strategic Policy Institute (ASPI), 12 June 2024. www.aspistrategist.org.au/russia-azerbaijan-exploit-new-caledonian-strife-against-france-china-stays-mum/
- Gray, C. S., 'Irregular Enemies and the Essence of Strategy: Can the American Way of War Adapt', US Army War College Press, 2006. <https://press.armywarcollege.edu/monographs/721/>
- Gray, C. S., 'Coping With Uncertainty: Dilemmas of Defense Planning. Comparative Strategy', Vol. 27, No. 4, 2008, pp. 324–331. <https://doi.org/10.1080/01495930802358414>
- Greene, S., Kagan, D., Boulègue, M., Ålander, M. & White, D., 'War Without End: Deterring Russia's Shadow War', Center for European Policy Analysis (CEPA), 31 March 2026. <https://cepa.org/comprehensive-reports/war-without-end-deterring-russias-shadow-war/>
- Gurcov, N., 'Testing the waters: Suspected Russian activity challenges Europe's support for Ukraine', Armed Conflict Location & Event Data (ACLED), 22 May 2025. <https://acleddata.com/report/testing-waters-suspected-russian-activity-challenges-europes-support-ukraine>
- Hathaway, O. A. & Shapiro, S. J., 'Might Unmakes Right – The Catastrophic Collapse of Norms Against the Use of Force', Foreign Affairs, July/August 2025. www.foreignaffairs.com/united-states/might-unmakes-right-hathaway-shapiro
- Heap, B. (Ed.), 'Strategic Communications Hybrid Threats Toolkit Published by the Nato Strategic Communications Centre of Excellence – Applying the principles of NATO Strategic Communications to understand and counter grey zone threats', NATO Strategic Communications Centre of Excellence, 2021. https://stratcomcoe.org/cuploads/pfiles/Strategic-Communications-Hybrid-threats-Toolkit_Rev_12L.pdf

- Hobbs, C. & Torreblanca, J. I., 'Byting back: The EU's digital alliance with Latin America and the Caribbean', European Power, European Council on Foreign Relations (ECFR), 24 October 2022. <https://ecfr.eu/publication/byting-back-the-eus-digital-alliance-with-latin-america-and-the-caribbean/>
- Hoffman, F. G., 'Conflict in the 21st Century: The Rise of Hybrid Wars', Potomac Institute for Policy Studies, December 2007. www.potomac institute.org/images/stories/publications/potomac_hybridwar_0108.pdf
- Hoffman, F. G., 'Assessing "Cognitive Warfare"', Small Wars Journal, 14 November 2025. <https://smallwarsjournal.com/2025/11/14/assessing-cognitive-warfare/>
- Hoffman, F. G., Email to Julien Theron, 28 August 2020.
- Höller, L., 'Researchers home in on origins of Russia's Baltic GPS jamming', DefenseNews, 02 July 2025. www.defensenews.com/global/europe/2025/07/02/researchers-home-in-on-origins-of-russias-baltic-gps-jamming/
- Higgins, J. C., 'Strategic Clarity: An Argument for Effective Deterrence', DKI APCSS, Perspectives, Vol.24, 23 June 2023. https://dkiapcss.edu/nexus_articles/strategic-clarity-an-argument-for-effective-deterrence/
- Huminski, J. C., 'Russia, Ukraine, and the Future Use of Strategic Intelligence', PRISM 10, No. 3, National Defence University Press, September 2023. https://ndupress.ndu.edu/Portals/68/Documents/prism/prism_10-3/prism_10-3_8-25_Huminski.pdf?ver=7kbBfjYhi02a14RjbWkhA%3D%3D
- Hybrid CoE (n.d.), Hybrid warfare, The European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE), no date. www.hybridcoe.fi/hybrid-warfare/
- Intelligence College in Europe, 'The College', no date. www.intelligence-college-europe.org/presentation/
- Interfax, 'Moscow preparing countermeasures against NATO in Baltics – Russian presidential aide', Military news, 18 February 2025. www.interfax-russia.ru/military/news_eng/419065
- Jakóbowski, J. & Oertel, J., 'Electric shock: The Chinese threat to Europe's industrial heartland', European Council on Foreign Relations (ECFR), Policy Brief, 15 May 2025. <https://ecfr.eu/publication/electric-shock-the-chinese-threat-to-europes-industrial-heartland/>
- Jalabert, Q., Van Puyvelde, D. & Maguire, T., 'Calling Out Russia: France's Shift on Public Attribution', War on the Rocks, 03 July 2025. <https://warontherocks.com/2025/07/calling-out-russia-frances-shift-on-public-attribution/>
- Jensen, B., 'Reindustrialization and Great Power Competition: Deterrence by Capacity, Center for Strategic and International Studies, 27 July 2026. www.csis.org/analysis/reindustrialization-and-great-power-competition-deterrence-capacity
- Jervis, R., Perceptions and Misperceptions in International politics, New edition, Princeton University Press, 2017
- Jochecová, K., 'Russia could start a major war in Europe within 5 years, Danish intelligence warns', Politico, 11 February 2025. www.politico.eu/article/russia-war-threat-europe-within-5-years-danish-intelligence-ddis-warns/
- Jones, S. G., 'Russia's Shadow War Against the West', Brief, Center for Strategic and International Studies (CSIS), 18 March 2025. www.csis.org/analysis/russias-shadow-war-against-west
- Jungwirth, R., Smith, H., Willkomm, E., Savolainen, J., Alonso Villota, M., Lebrun, M., Aho, A., Giannopoulos, G., Hybrid Threats: A Comprehensive Resilience Ecosystem, Publications Office of the European Union, Luxembourg, 2023. https://doi.org/10.2760/37899_JRC129019
- Kaushal, S., 'All Strategies Short of War: Getting the Most Out of the Gray Zone', Modern War Institute, 28 February 2022. <https://mwi.westpoint.edu/all-strategies-short-of-war-getting-the-most-out-of-the-gray-zone/>

- Keršanskas (2020a), V., 'Hybrid CoE launches a playbook on hybrid deterrence', European Centre of Excellence for Countering Hybrid Treats (Hybrid CoE), 09 March 2020. www.hybridcoe.fi/news/hybrid-coe-launches-a-playbook-on-hybrid-deterrence/
- Keršanskas (2020b), V., 'DETERRENCE: Proposing a more strategic approach to countering hybrid threats', European Centre of Excellence for Countering Hybrid Treats (Hybrid CoE), Hybrid CoE Paper 2, March 2020. www.hybridcoe.fi/wp-content/uploads/2020/07/Deterrence_public.pdf
- Keršanskas, V., 'Deterring disinformation? Lessons from Lithuania's countermeasures since 2014', European Centre of Excellence for Countering Hybrid Treats (Hybrid CoE), Hybrid CoE Paper 6, April 2021. www.hybridcoe.fi/wp-content/uploads/2021/04/20210427_Hybrid-CoE-Paper-6_Deterring_disinformation_WEB.pdf
- Kertysova, K. & Gricius, G., 'Countering Russia's Hybrid Threats in the Arctic', European Leadership Network, August 2023. www.europeanleadershipnetwork.org/wp-content/uploads/2023/12/23_11_22_Countering-Russias-Hybrid-threats-in-the-Arctic15_ES_EK40.pdf
- Khan, S., 'Russia's Suspected 'Hybrid War' Tests Europe's Air Defences', Modern Diplomacy, 05 November 2025. <https://moderndiplomacy.eu/2025/11/05/russias-suspected-hybrid-war-tests-europes-air-defences/>
- Khrebet, A., 'Warsaw to 'demand explanations' from Moscow after Russian missile entered Polish airspace', The Kyiv Independent, 24 March 2024. <https://kyivindependent.com/poland-to-demand-explanations-from-russia-after-missile-aimed-at-ukraine-violated-polish-airspace/>
- Kitzen, M. & van Kuijk, C., 'All Deterrence Is Local: The Utility and Application of Localised Deterrence in Counterinsurgency', In: Osinga, F. & Sweijs, T. (Eds.), NL ARMS Netherlands Annual Review of Military Studies 2020: Deterrence in the 21st Century – Insights from Theory and Practice, pp. 287–310, Springer, 2021. https://doi.org/10.1007/978-94-6265-419-8_15
- Knopf, J. W., 'The Fourth Wave in Deterrence Research', Contemporary Security Policy, Vol. 31, No 1, 1 April 2010, pp. 1–33. <https://doi.org/10.1080/13523261003640819>
- Kremidas-Courtney, C., 'Beyond the Wagner virus: hybrid threats in Africa', Friends of Europe, 12 July 2023. www.friendsofeurope.org/insights/critical-thinking-beyond-the-wagner-virus-hybrid-threats-in-africa/
- Lafont Rapnouil, M., 'The Brutalization of Diplomacy?', The Hague Journal of Diplomacy, Vol. 19, No. 4, pp. 726–736. <https://doi.org/10.1163/1871191x-20241542>
- Latvian Ministry of Foreign Affairs, 'Latvia's chairmanship of the Baltic Council of Ministers in 2025', 02 January 2025. www.mfa.gov.lv/en/article/latvias-chairmanship-baltic-council-ministers-2025
- Liddell Hart, B. H., Strategy, Second Revised Edition, 1991.
- LSM English, 'Latvian PM Silīņa stresses defense industry development in address to parliament', Latvian Public Service Media (LSM), 13 March 2025. <https://eng.lsm.lv/article/politics/saeima/13.03.2025-latvian-pm-silina-stresses-defense-industry-development-in-address-to-parliament.a590716/>
- Madhani, A. & Moulson, G., 'Russian assassination plots against those supporting Ukraine uncovered in Europe, official says', The Associated Press, 12 July 2024. <https://apnews.com/article/germany-russia-threats-report-rheinmetall-plot-2cee42e9f9f6940eb960b0b052e3e670>
- Marleku, A., 'Public intelligence as a strategic tool: The role of real-time intelligence disclosure in the Ukraine War', Security & Defence Quarterly, Vol. 50, No. 2, 30 June 2025. <https://securityanddefence.pl/pdf-205566-127235?filename=Public%20intelligence%20as%20a.pdf>
- Martisiute, M., 'Flying blind: How to prevent Russian GPS operations from causing a European air disaster?', Discussion Paper, Europe in the World Programme, European Policy Centre, 11 November 2025. <https://d1xp398qalq39s.cloudfront.net/uploads/ckeditor/2025/11/10/gps-dp-v4.pdf>

- Marzano, J., 'Cyberattacks and Infowarfare Targeting Milano–Cortina 2026. Anatomy of a Hybrid Campaign', Decode 39, 03 March 2026. <https://decode39.com/13729/cyberattacks-and-infowarfare-targeting-milano-cortina-2026-anatomy-of-a-hybrid-campaign/>
- Mazarr, M. J., 'Understanding Deterrence', Perspective, Rand Corporation, 2018. https://www.rand.org/content/dam/rand/pubs/perspectives/PE200/PE295/RAND_PE295.pdf
- McChrystal, S., Collins, T., Silverman, D. & Fussell, C., Team of Teams – New Rules of Engagement for a Complex World, Portfolio Penguin, 2015.
- McClenon, J. M., 'We're WEIRD and Our Adversaries Know It: Psychological Biases Leave the United States Vulnerable to Cognitive Domain Operations', Irregular Warfare Initiative, 07 June 2023. <https://irregularwarfare.org/articles/were-weird-and-our-adversaries-know-it-psychological-biases-leave-the-united-states-vulnerable-to-cognitive-domain-operations/>
- Messmer, M. & Bego, K., 'Global security continued to unravel in 2025. Crucial tests are coming in 2026', Expert Comment, Chatham House, 12 December 2025. www.chathamhouse.org/2025/12/global-security-continued-unravel-2025-crucial-tests-are-coming-2026
- Michaels, J. H., 'Deterrence Warning Messages – A Short Guide for NATO', The Hague Centre for Strategic Studies (HCSS), June 2025. <https://hcss.nl/report/deterrence-warning-messages-a-short-guide-for-nato/>
- Ministry of Defence of the Republic of Latvia, 'What To Do in Case of a Crisis', Updated Edition 2022. www.jelgava.lv/wp-content/uploads/2023/06/72hours.pdf
- Monaghan, S. 'Hybrid CoE Paper 12: Deterring Hybrid Threats: Towards a Fifth Wave of Deterrence Theory and Practice', European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE), March 2022. <https://www.hybridcoe.fi/publications/hybrid-coe-paper-12-deterring-hybrid-threats-towards-a-fifth-wave-of-deterrence-theory-and-practice/>
- Monaghan, S., Cullen, P. & Wegge, N., 'MCDC Countering Hybrid Warfare Project: Countering Hybrid Warfare, Multinational Capability Development Campaign (MCDC)', March 2019. https://assets.publishing.service.gov.uk/media/5c8141e2e5274a2a51ac0b34/concepts_mcdc_countering_hybrid_warfare.pdf
- Muhić, E., 'Transforming the Intelligence Cycle through Adapting to Complex Environments and the Operational Dynamics of Special Warfare, Applied Cybersecurity & Internet Governance, Vol. 4, No. 1, 2025. <https://doi.org/10.60097/ACIG/211788>
- Musland, L. 'A2/AD and the missile threat – systems, countermeasures and models', FFI report 21/00638, Norwegian Defence Research Establishment (FFI), 12 March 2021. www.ffi.no/en/publications-archive/a2-ad-and-the-missile-threat-systems-countermeasures-and-models
- Ngendakumana, P.-E., 'Germany must be ready for war by 2029, defense minister warns', Politico, 05 June 2024. www.politico.eu/article/germany-must-be-ready-for-war-by-2029-defense-minister-warns/
- Niinistö, S., 'Safer Together Strengthening Europe's Civilian and Military Preparedness and Readiness', Report by Sauli Niinistö, former President of the Republic of Finland, In his capacity as Special Adviser to the President of the European Commission, 2024. https://commission.europa.eu/document/download/5bb2881f-9e29-42f2-8b77-8739b19d047c_en?filename=2024_Niinisto-report_Book_VF.pdf
- Nord, M., Altman, D. Angiolillo, F., Fernandes, T., Good God, A. & Lindberg, S. I., 'Democracy Report 2025: 25 Years of Autocratization – Democracy Trumped?', University of Gothenburg: V-Dem Institute, March 2025. www.v-dem.net/documents/60/V-dem-dr_2025_lowres.pdf
- Nordic Defence Cooperation, 'Vision for Nordic Defence Cooperation' (alias 'Vision 2030'), 30 April 2024. www.nordefco.org/files/NORDEFCO-vision-2030-.pdf
- Norwegian Directorate for Civil Protection (DSB), 'How You Can Play Your Part in Norway's Emergency Preparedness', no date. www.dsb.no/siteassets/sikkerhverdag/egenberedskap/brosjyren/dsb-egenberedskap-engelsk-web.pdf

Office of the President of the Republic of Lithuania, 'Address by Gitanas Nausėda, President of the Republic of Lithuania, at the conference "Russia's hybrid war against the democratic world. A challenge for European remembrance policy"', 17 November 2022. <https://lrp.lt/en/address-by-gitanas-nauseda-president-of-the-republic-of-lithuania-at-the-conference-russias-hybrid-war-against-the-democratic-world.-a-challenge-for-european-remembrance-policy/39477>

Østhagen, A., 'The Arctic after Russia's invasion of Ukraine: The increased risk of conflict and hybrid threats, Hybrid CoE Paper 18, May 2023. www.hybridcoe.fi/wp-content/uploads/2023/05/20230510-Hybrid-CoE-Paper-18-Arctic-after-Ukraine-WEB.pdf

Päästeamet – Estonian Rescue Board, 'What To Do in a Crisis Situation – Be Prepared!', Update version, 2022. www.rescue.ee/files/2022-10/ole-valmis-2022-eng.pdf?fb0999f82d

Pabriks, A., 'Artis Pabriks: The role of intelligence for successful governance', Centrum Balticum, 22 January 2026. <https://centrumbalticum.org/artis-pabriks-the-role-of-intelligence-for-successful-governance>

Pernik, P., 'Cyber deterrence: A case study on Estonia's policies and practice', Hybrid CoE Paper 8, European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE), October 2021. www.hybridcoe.fi/wp-content/uploads/2021/10/20211012_Hybrid_CoE_Paper_8_Cyber_deterrence_WEB.pdf

Polish Government Centre for Security, 'Get Ready! Guide for Crisis and War', 2022. www.gov.pl/attachment/ac2c8078-d67f-4d07-a10e-15da398df799

Popescu, N., 'Hybrid tactics: Russia and the West', Issue Alert 46, European Union Institute for Security Studies (EUISS), October 2015. www.iss.europa.eu/sites/default/files/EUISSFiles/Alert_46_Hybrid_Russia.pdf

Popescu-Zamfir, O., 'Russian Interference: Coming Soon to an Election Near You', Carnegie Europe, 13 February 2025. <https://carnegieendowment.org/europe/strategic-europe/2025/02/russian-interference-coming-soon-to-an-election-near-you>

President of the Republic of Poland, 'Joint statement by the Presidents of Lithuania, Poland and Ukraine', 02 December 2021. www.president.pl/archives/andrzej-duda/news/joint-statement-by-the-presidents-of-lithuania-poland-and-ukraine.45908

Rauta, V., 'Countering state-sponsored proxies: Designing a robust policy', Hybrid CoE Paper 23, European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE), February 2025. www.hybridcoe.fi/wp-content/uploads/2025/02/web_Hybrid_CoE_Paper-23_rgb.pdf

Rekawek, K., Lanchès, J., Zotova, M., Hajdu, D., Bowser, D., 'Russia's Crime-Terror Nexus- Criminality as a Tool of Hybrid Warfare in Europe', Globsec, 30 September 2025. www.globsec.org/what-we-do/publications/russias-crime-terror-nexus-criminality-tool-hybrid-warfare-europe

Reuters (2025a), 'EU's Kallas: Russia is posing an existential threat to our security', Reuters, 22 January 2025. www.reuters.com/world/europe/eus-kallas-russia-is-posing-an-existential-threat-our-security-2025-01-22/

Reuters (2025b), 'Europe 'no longer at peace' with Russia, says Germany's Merz', 29 September 2025. www.reuters.com/world/europe-no-longer-peace-with-russia-says-germanys-merz-2025-09-29/

Roberts, S., 'Hybrid CoE attending the OSCE ASRC Side Event on Countering Hybrid Threats', European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE), 26 June 2019. www.hybridcoe.fi/news/hybrid-coe-attending-the-osce-asrc-side-event-on-countering-hybrid-threats/

Rogozińska, A., 'Evolution of the Russian information warfare in the wake of the invasion of Ukraine', Defence24, 17 January 2026. <https://defence24.com/analysis/evolution-of-the-russian-information-warfare-in-the-wake-of-the-invasion-of-ukraine>

Rusinaitė, V., 'Turning strategy into praxis: Lessons in hybrid threat deterrence', Hybrid CoE Paper 25, , European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE), August 2025. www.hybridcoe.fi/wp-content/uploads/2025/08/Hybrid-CoE-Paper-25-Turning-strategy-into-praxis-web.pdf

- Salisbury, D., 'Drones targeting European nuclear weapons infrastructure', The International Institute for Strategic Studies (IISS), 12 December 2025. www.iiiss.org/online-analysis/online-analysis/2025/12/drones-targeting-european-nuclear-weapons-infrastructure/
- Sari, A., 'Legal resilience in an era of grey zone conflicts and hybrid threats', Cambridge Review of International Affairs, Vol. 33, No. 6, 20 May 2020, pp. 846–867. <https://doi.org/10.1080/09557571.2020.1752147>
- Savitz, S., 'Uncrewed maritime vessels: Shaping naval power in hybrid threat operations', Hybrid CoE Working Paper 34, European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE), October 2024. www.hybridcoe.fi/wp-content/uploads/2024/10/20241007-Hybrid-CoE-Working-Paper-34-Uncrewed-maritime-vessels-WEB.pdf
- Savolainen, J., 'Suuremman häiriön mahdollisuus – Korkean intensiteetin hybridioperaatio', In: Hallikainen, I. & Savolainen, J., Ilkeyksiä, sabotaasia, hyökkäyksiä, Otava, 2025.
- Schelling, T. C., The Strategy of Conflict, Harvard University Press, 1980.
- Shagina, M., 'Sanctions against Russia: The West needs a grand strategy', Hybrid CoE Strategic Analysis 32, European Centre of Excellence for Countering Hybrid Treats (Hybrid CoE), May 2022. www.hybridcoe.fi/wp-content/uploads/2022/05/20220519-Hybrid-CoE-Strategic-Analysis-32-Sanctions-against-Russia-WEB.pdf
- Shagina, M., 'Lessons learned from Western sanctions on Russia: Knowing your target well', Hybrid CoE Strategic Analysis 35, Hybrid CoE Strategic Analysis 9, European Centre of Excellence for Countering Hybrid Treats (Hybrid CoE), September 2024. www.hybridcoe.fi/wp-content/uploads/2024/09/20240916-Hybrid-CoE-Strategic-Analysis-35-WEB.pdf
- Shahbazov, F., 'The Acceleration of Putin's Shadow War', Center for European Policy Analysis (CEPA) 01 October 2025. <https://cepa.org/article/the-acceleration-of-putins-shadow-war/>
- Siebold, S., 'Germany at risk of violent conflict with Russia, intelligence chief says', Reuters, 05 October 2026. www.reuters.com/business/finance/germany-risk-violent-conflict-with-russia-intel-chief-says-2026-10-05/
- Snyder, G. H., Deterrence and Defense – Toward a Theory of National Security, Princeton Legacy Library, Princeton University Press, 2016
- Snyder, R., 'Kyiv as the New Berlin: Ukraine's Role in Modern Espionage Conflict', Small Wars Journal, 22 July 2025. <https://smallwarsjournal.com/2025/07/22/kyiv-as-the-new-berlin-ukraine-role-in-modern-espionage-conflict/>
- Starcevic, S., 'Europe is at hybrid war, Danish prime minister announces', Politico, 26 September 2025. www.politico.eu/article/europe-hybrid-war-danish-prime-minister-says-russia-drones/
- Stijnman, E., 'Countering Russian hybrid warfare – The best defence is a good offense', Clingendael Alert, Clingendael – Netherlands Institute of International Relations, July 2025. www.clingendael.org/sites/default/files/2025-07/Countering_Russian_hybrid_warfare.pdf
- Stubb, A., 'The West's Last Chance – How to Build a New Global Order Before It's Too Late', Foreign Affairs, 02 December 2025. www.foreignaffairs.com/united-states/wests-last-chance
- Swedish Psychological Defence Agency (MPF), 'Our mission', no date, <https://mpf.se/psychological-defence-agency/about-us/our-mission>
- Sytas, A., 'Lithuania blames Russia for IKEA arson, notes store logo matches Ukraine's colours', Reuters, 17 March 2025. www.reuters.com/world/europe/lithuania-says-russian-military-intelligence-was-behind-ikea-arson-last-year-2025-03-17/
- Taddeo, M., 'How to Deter in Cyberspace', Hybrid CoE Strategic Analysis 9, European Centre of Excellence for Countering Hybrid Treats (Hybrid CoE), June–July 2018. www.hybridcoe.fi/wp-content/uploads/2020/07/Strategic-Analysis-9-Taddeo.pdf

- Telegrafi, 'The Netherlands prepares for a possible war with Russia', Telegrafi, 08 May 2025. <https://telegrafi.com/en/holanda-pergatitet-per-nje-lufte-te-mundshme-rusine/>
- Theron, J., 'Networks of Threats: Interconnection, Interaction, Intermediation', Journal of Strategic Security, Vol. 14, No. 3, 2021. <https://doi.org/10.5038/1944-0472.14.3.1942>
- Theron, J., 'Lower Spectrum Conflict Mechanisms', In: Mölder, H., Voinea, C.F., Sazonov, V. (eds) Producing Cultural Change in Political Communities, Contributions to Political Science, Springer, 2023. https://doi.org/10.1007/978-3-031-43440-2_3
- The Swedish Civil Contingencies Agency (MSB), 'In Case of Crisis or War', November 2024. <https://rib.msb.se/filer/pdf/30874.pdf>
- Tor, U., '“Cumulative Deterrence” as a New Paradigm for Cyber Deterrence', Journal of Strategic Studies, Vol. 40, No 1–2, 02 January 2017, pp. 92–117. <https://www.tandfonline.com/doi/full/10.1080/01402390.2015.1115975>
- United Nations General Assembly, 'Resolution adopted by the General Assembly [on the report of the Sixth Committee (A/56/589 and Corr.1)]', A/RES/56/83, 28 January 2002. <https://docs.un.org/en/a/RES/56/83>
- United States Department of Defense, '2022 National Defense Strategy of the United States of America, including the 2022 Nuclear Posture Review and the 2022 Missile Defense Review', October 2022. <https://media.defense.gov/2022/Oct/27/2003103845/-1/-1/2022-NATIONAL-DEFENSE-STRATEGY-NPR-MDR.PDF>
- van den Berg, B. & Stijnman, E., 'What the Russian drone incursion into Poland means for NATO Testing the threshold', Clingendael, 23 September 2025. www.clingendael.org/publication/what-russian-drone-incursion-poland-means-nato
- Vasques, E., 'Russia's hybrid war is the new normal, says Finnish president', Euronews, 15 January 2025. www.euronews.com/my-europe/2025/01/15/russias-hybrid-war-is-the-new-normal-says-finnish-president-radio-schuman
- Warsaw Security Forum, 'Winning the War Before the War A Blueprint for Europe', Warsaw Security Forum Report 2025, 2025. <https://warsawsecurityforum.org/wp-content/uploads/2025/09/WSF-Report-2025-WEB-v2.pdf>
- Weiss, M & Kopaleishvili, K., with Flis, D., Gielewska, A., Morozova, A., Pawłowska, A., Sprinße, I., Makaraitytė, I., Roonemaa, H. & Grozev, C., 'How Russia's GRU Plotted Europe's Parcel Explosions', VSquare, 17 September 2025. <https://vsquare.org/revealed-how-russia-gru-plotted-europe-parcel-explosions/>
- Whitehead, J., 'Poland accuses Russia of arson over 2024 shopping centre fire', BBC, 12 May 2025. www.bbc.com/news/articles/cgegjlrvq84o
- Wigell, M., 'Democratic Deterrence – How to Dissuade Hybrid Interference', Working Paper 110, Finnish Institute of International Affairs (FIIA), september 2019. <https://fii.fi/wp-content/uploads/2019/09/wp110-democratic-deterrence.pdf>
- Wiseman, K., 'Russia is expanding its espionage output at a 'staggeringly reckless' rate. Here's why', Australian Broadcasting Corporation (ABC), 30 May 2025. www.abc.net.au/news/2025-05-31/russia-spy-espionage-network-expanding/105297530
- Yle News/STT, 'Finnish PM urges EU states to 'show solidarity with Eastern and Northern European countries'', Yle, 01 October 2025. <https://yle.fi/a/74-20186153>
- Zegart, A., 'Open Secrets – Ukraine and the Next Intelligence Revolution', Foreign Affairs, 20 December 2022. www.foreignaffairs.com/world/open-secrets-ukraine-intelligence-revolution-amy-zegart
- Zysk, K., 'Written evidence (ARC0016)', UK Parliament, House of Lords International Relations and Defence Committee, 03 May 2023. <https://committees.parliament.uk/writtenevidence/121959/pdf/>

LIST OF ABBREVIATIONS

A2/AD: anti-access / area denial	EUISS: European Union Institute for Security Studies	LILP: Low impact, low probability
AI: artificial intelligence	EUMC: European Union Military Committee	MPCC: EU Military Planning and Conduct Capability's
ARISWA: Articles on the Responsibility of States for Internationally Wrongful Acts	EUMS: European Union Military Staff	MPF: Swedish Psychological Defence Agency
BAMAD: German Federal Office of Military Counter-Intelligence	EUMS INT: European Union Military Staff Intelligence Directorate	NATO: North Atlantic Treaty Organization
BfV: German Federal Office for the Protection of the Constitution	EU MS: European Union Member States	OHQ: European Union Operation Headquarters
BMS: Battlefield management system	EU RDC: European Union Rapid Deployment Capacity	OSINT: open-source intelligence
BND: German Federal Intelligence Service	EW: Electronic warfare	PACE: EU–NATO Parallel and Coordinated Exercise
CBRN: chemical, biological, radiological and nuclear	EZE: end-to-end encryption	PSC: Political and Security Committee
CER: Critical Entities Resilience	FIMI: foreign information manipulations and interference	P2P-E: Peer-to-peer encrypted communication
CFSP: Common Foreign and Security Policy	GNSS: Global navigation satellite system	RD strategy: resilience–deterrence strategy
CI: Critical infrastructure	HFC: Hybrid Fusion Cell	SatCen: European Union Satellite Centre
CORE (exercise): EU-NATO Coherent Resilience	HIHP: High impact, high probability	SIAC: Single Intelligence Analysis Capacity
CORE (model): comprehensive resilience ecosystem	HILP: High impact, low probability	TEU: Treaty on European Union
Coreper: Committee of the permanent representatives	HR/VP: High Representative of the Union for Foreign Affairs and Security Policy/Vice-President of the European Commission	TFEU: Treaty on the Functioning of the European Union
CUI: Critical underwater infrastructure	HWP ERCHT: Horizontal Working Party on Enhancing Resilience and Countering Hybrid Threats	TTX: Tabletop exercise
C2: Command and control	Hybrid CoE: European Centre of Excellence for Countering Hybrid Threats	UAS: Unmanned aerial systems
C-UAV	ICC: International Criminal Court	UAV
DID: detection–identification–determination	ICE: Intelligence College in Europe	UCPM: Union Civil Protection Mechanism
EDTIB: European Defence Technology Industrial Base	ICJ: International Court of Justice	UGV: Unmanned ground vehicle
EEAS: European External Action Service	ILC: UN International Law Commission	USSR: Union of Soviet Socialist Republics
ESPAS: European Strategy and Policy Analysis System	IPCR: Integrated Political Crisis Response	USV: Unmanned surface vehicles
ESS: European security ecosystem	ISACs: Information Sharing and Analysis Centres JRC: European Commission Joint Research Centre	UUV:
EU: European Union	LIHP: Low impact, high probability	VLOPs: Very large online platforms
EU INTcen: European Union Intelligence and Situation Centre		VLOSEs: Very large online search engines
		VPN: Virtual private networks

LIST OF FIGURES

Figure 1. Multi-actor saturation of the European security ecosystem	12
Figure 2. Exploitation of attacks resulting in cascading effects	13
Figure 3: Hybrid threat operations' escalation to hybrid warfare	16
Figure 4. Operational resilience against hybrid threats	20
Figure 5. Deterrence by denial	23
Figure 6. Deterrence by punishment	23
Figure 7. Absolute deterrence based on the anticipation of future operations	24
Figure 8. Restrictive deterrence, decreasing the intensity of the hybrid threat operation	25
Figure 9. Cumulative deterrence, limiting hostile operations to a tolerable minimum	25
Figure 10. Deterrence by disclosure, publicly revealing hybrid threat operations at an early stage to undermine them	25
Figure 11. Deterrence by stratcom	26
Figure 12. Integrated deterrence, preventing an attack by preventively scaling multiple capabilities	26
Figure 13. Internalised deterrence: hoarding dissuading capabilities to lower the need for strong acts of deterrence	26
Figure 14. Extended deterrence: collectively shielding an attacked ally	27
Figure 15. Deterrence by inducement to deviate hybrid threat operations' harmful trajectories to better defended area	27
Figure 16. The relationship between resilience and deterrence	32
Figure 17. Possibilities of resilience and deterrence to counter hybrid threat operations	33
Figure 18: Societal collapse due to insufficient resilience and the absence of deterrence	35
Figure 19: Cumulated effect of deterrence and resilience on hybrid threat operations	35
Figure 20: Proactive anticipation	38
Figure 21. Vague attribution	43
Figure 22. Strong attribution	43
Figure 23. Active defence	44
Figure 24. Reactive response	46
Figure 25. Resilience–deterrence strategy	48
Figure 26. Case study 1: Resilience only	50
Figure 27. Case study 2: Resilience and deterrence by denial	51
Figure 28. Case study 3: Resilience and deterrence by punishment against a high-impact operation	52
Figure 29. Case study 4: Resilience and deterrence by disclosure with early detection against a high-impact operation	53

LIST OF TABLES

Table 1: Different types of hybrid threat operations and possible combinations of deterrence and resilience for proactive anticipation	36
Table 2: Means to improve proactive anticipation	37
Table 3: Options to develop deterrence and resilience capacities through practice, simulation and guidance	37
Table 4: RD strategy's risks and mitigations	49

ANNEXES 1:

MEASURES FOR RESILIENCE

This annex proposes a non-exhaustive list of possible operational measures for resilience to be developed or further implemented at the EU and national levels. Many of the measures listed here already exist through EU action, including legislative measures, or have been announced.

Based on the CORE model and the RD strategy, the intent of these non-exhaustive and indicative set of operational measures is to point out specific means of countering hybrid warfare through a whole-of-society practical implementation. The operational reinforcement of the resilience pillar contributes to enhancing proactive anticipation and active defence.

Resilience in the civic space

Education

1. Support independent research as a cornerstone of political sovereignty and economic development.
2. Promote interdisciplinary and transdisciplinary research to close knowledge gaps in studies related to hybrid threat operations, break down silos and foster innovations that secure interdependencies.
3. Introduce media literacy programmes for all ages, beginning with the youngest pupils in schools.
4. Strengthen academic institutions by promoting analytical skills, critical thinking and respectful argumentation.
5. Develop educational programmes that inform pupils, students and professionals about the risks, potential and operating mechanisms of AI.
6. Use the education system to identify the vulnerabilities of young people and devise appropriate mitigation measures.
7. Launch public, multi-support awareness campaigns on hybrid threat operations in general and on specific hostile hybrid campaigns for exemplification.
8. Audit and ensure research security, including the use of the European Commission's toolkit against foreign interference in research and innovation (European Commission, 2022).
9. Protect academic environments from malicious activities such as disinformation, propaganda and intelligence-gathering operations targeting the scientific community and students.
10. Implement democratic dialogue and anti-radicalisation programmes for young people in schools and universities while informing them about the dangers of polarisation.

Information

- 11.** Run information campaigns on international security developments and the stakes for democracies.
- 12.** Inform the public through dedicated threat assessments on a regular basis within the frameworks of authorities' strategic communication.
- 13.** Facilitate the threat awareness of public officials, scientists and journalists.
- 14.** Safeguard and support independent investigative journalism.
- 15.** Uphold ethics and deontology in journalism, with media watchdog bodies imposing strict penalties for misconduct related to disinformation and calls for hatred or violence.
- 16.** Introduce strict, cutting-edge measures to curb the spread of hatred and political polarisation on social media platforms.
- 17.** Protect citizens' privacy regarding the collection of user data, user profiling, algorithmic optimisation and the use of AI.
- 18.** Provide users with pedagogical guidance and practical tools to enhance the protection of their privacy.
- 19.** Employ AI to survey hybrid threat campaigns that seek to exert cognitive influence over society, security-defence apparatuses and decision-makers.
- 20.** Develop legal instruments and technological tools to ensure free and fair information, preventing external manipulation of elections.
- 21.** Establish a legal framework for doctored content on social media to restrict cognitive manipulation.
- 22.** Allow the possible suspension of social media services when democratic processes are under attack.
- 23.** Ensure the independence of media organisations (European Broadcasting Union, 2025b).
- 24.** Apply measures supported by the European Democracy Action Plan (European Commission, 2020b), the Rule of Law Report (European Commission, 2025e), the Code of Conduct on Disinformation (European Commission, 2025f) and the European Democracy Shield (European Parliament, 2025b).

Participation

- 25.** Include the civic space in major legislative work throughout the drafting and implementation of key laws.
- 26.** Support awareness programmes on resilience against hybrid threat operations, with clear, accessible information, conceived and implemented by the civic space and tailored for each type of public.
- 27.** Back civil-society training programmes for citizens to prepare them for hybrid threat operations, particularly HIOs.
- 28.** Finance and support investigative journalism and its networks by allocating resources to independent news outlets that expose hostile activities and disinformation campaigns.
- 29.** Fund, support and empower researchers and research networks on hybrid threats in Member States, across the EU and with democratic partners. Ensure that research findings, success factors and innovations are incorporated into institutional frameworks and communicated to the wider public via the media.
- 30.** Develop financial and political backing for civil-society initiatives countering hybrid threat operations in all 13 domains, and especially in the information, cyber, social/societal, cultural, political and military defence domains. Provide sustained funding where necessary.
- 31.** Integrate the civic and services spaces into lawmaking through a transdisciplinary approach to co-designing policies that address countering hybrid threat operations.

Resilience in the governance space

Whole of government

1. Ensure secure, cross-cutting, efficient and autonomous communication among inter-agency and intergovernmental networks.
2. Coordinate detection and identification capabilities for hybrid threat operations across government departments.
3. Treat hybrid threats systematically as structural and existential risks in both general and domain-specific policymaking.
4. Improve information sharing between institutions, bodies and agencies.
5. Strengthen the European security and defence technological and industrial ecosystem, including small and medium-sized enterprises, start-ups, research and technology organisations and larger industrial actors, with particular attention to technologies and capabilities relevant to civil security, critical entities and the continuity of essential services.
6. Include regular debriefs on hybrid threat operations in Member States' councils of ministers.
7. Systemise hybrid threat debriefs at working parties and committees, as well as at the levels of Committee of the permanent representatives (Coreper) and Council of the European Union.
8. Develop domain-specific hybrid threat expertise and facilitate these experts' institutional mobility so they can sensitise all institutions, bodies and agencies to rapidly changing requirements.
9. Foster an institutional culture of foresight on hybrid threats through regular training and exercises, including the identification of complex scenarios, at the local, national and European levels and with non-European partners.
10. Generalise the use of practice, simulations and guidance for public officials and services on hybrid threats, including regular domain-specific and multi-domain tabletop exercises (TTX) at the national and European levels, based on future disruptive strategies and HIOs.

Social contract

11. Maintain open communication with all stakeholders from the civic, governance and services sectors to determine the nature and scope of hybrid threat operations.
12. Facilitate exchanges with associations, trade unions and corporations, and incorporate their viewpoints into the drafting of major legislative proposals intending to counter hybrid threat operations.
13. Support the civic and services spaces in developing high-tech, mid-tech, low-tech and no-tech tools to counter operations across all domains. Ensure assistance is agile, fast-tracked and scalable, promoting the development of tools in line with the development of threats. Consider establishing a dedicated cross-domain public agency for this purpose.
14. Establish structured cooperation mechanisms bringing together public authorities, practitioners, critical entities, research and technology organisations, universities, small and medium-sized enterprise (SMEs), start-ups and larger industrial actors to co-design, develop, test and validate solutions to identified operational needs and future hybrid threat scenarios.
15. Integrate the civic and services spaces into strategic foresight activities, simulations and practical exercises.
16. Organise regular conferences in EU MS that bring together civic, governance and services representatives to discuss national and European security, with a focus on the changing nature of hybrid threats. Use these events to enhance situational awareness among analysts, scholars, practitioners and decision-makers and help identify new countering actors, tools, measures and best practices.

Preparedness and response

17. Monitor rigorously and assess the efficiency of measures so that they can be adjusted swiftly.

- 18.** Develop networks of indicators to improve the detection of hybrid threat operations across all institutions, bodies and agencies, specific to every domain and centralised by the government.
- 19.** Centralise post-analysis information at the strategic/policy level into a single body to ease determination in each EU MS, with the body identified as the key interlocutor for other Member States and partners.
- 20.** Boost capabilities to identify hybrid threat operations in all sectors, especially in the most challenging areas, such as the intelligence, political, economic, social/societal and cultural domains.
- 21.** Fast-track impact-driven measures and legislation aimed at countering hybrid threat operations to prevent strategic adaptation from becoming obsolete.
- 22.** Implement and enforce laws concerning hybrid threat operations, incorporating severe penalties for breaches, particularly in the information, political, intelligence and economic domains, applicable to both domestic and foreign actors.
- 23.** Continuously monitor and measure the effectiveness of hybrid threat measures and legislation, and adapt them promptly when expected outcomes are not achieved, including in response to emerging vulnerabilities or adversary adaptations.
- 24.** In addition to intelligence sharing, enhance collective capabilities for determination.
- 25.** Develop and expand the mobilisation of cross-domain EU HRRT.

Trust building

- 26.** Treat attribution as a strategic necessity, ensuring enhanced options for reactive response. Make sure that citizens are fully informed of the situation and that society can respond appropriately.
- 27.** Enhance transparency and accountability in decision-making by clarifying the context, processes and outcomes of the reactive response implemented to deter hybrid threat operations.
- 28.** Develop systematic ethical and deontological frameworks – through legislation, guiding tools and best-practice procedures – to counter hybrid threats and prevent any anti-democratic use by public, private, domestic or foreign actors.

Resilience in the services space

Investments

- 1.** Facilitate investments in security and defence through loans, direct public funding and foreign direct investment of democratic partners.
- 2.** Enable the creation of large European defence companies by promoting partnerships, mergers and acquisitions, with clearly defined roles for each participant.
- 3.** Expand investment in the European Defence Technology Industrial Base (EDTIB), including in partner EU MS, especially those that lack a strong domestic industry.
- 4.** Provide robust financial support and streamline bureaucracy for emerging security- and defence-related technologies, whether high-, mid- or low-tech.
- 5.** Invest in research that deepens the theoretical and applied understanding of interconnected infrastructure systems.
- 6.** Modernise critical entities and critical infrastructure when necessary to make them more resilient against future operations.
- 7.** Build strategic stockpiles of essential goods and supplies (e.g. food, water, energy, medical supplies), at the local, national and European levels, in accordance with planification policies, to lessen dependencies.
- 8.** Invest in and promote cybersecurity solutions for both citizens and businesses.
- 9.** Construct European data centres with a high level of physical and digital protection to ensure strategic autonomy.
- 10.** Invest in European chips, operating systems, interfaces and software solutions.

Public–private partnerships

- 11.** Introduce measures that build public trust and diminish societal polarisation.
- 12.** Foster public–private cooperation to break down sectoral silos and increase the flexibility of interdependencies.
- 13.** Implement mutual aid agreements to enable a faster response to disruptive events within the EU and with democratic partners.
- 14.** Adapt deployable response capabilities able to cope with the increasing threat environment.
- 15.** Identify and develop tools for detecting and identifying signals across all domains, through public–private collaboration and a regional systemic approach.
- 16.** Create comprehensive instruments for strategic-level determination analysis of hybrid threat operations, including – but not limited to – advanced AI and AI-enabled facilitation methods, following robust feasibility and risk mitigation studies safeguarding the use of the technology.
- 17.** Facilitate the application of national and European legislation by the services space – particularly in the infrastructure, cyber and economic domains – to enhance resilience, streamlining procedures and reducing bureaucratic burdens.
- 18.** Develop indicators to measure resilience in each domain and at the national level, incorporating potential cascading effects and their weaponisation, and conduct regular evaluations based on these indicators.
- 19.** Ensure the resilience and protection of the physical, cyber and functional aspects of critical entities.
- 20.** Assess cross-border and cross-sector interdependencies at the regional and European levels.
- 21.** Identify vulnerabilities in and safeguard supply chains that are vital for security, defence and essential services.
- 22.** Secure open communication regarding private sector needs and adapt public administrative processes as far as possible to meet those requirements.

Supply of goods

- 23.** Ensure global access to raw materials and resources.
- 24.** Diversify key supply sources and chains to reduce reliance on single sources.
- 25.** Restore and strengthen European production capacities and reduce critical dependencies in strategically relevant technologies, products, services and supply chains.
- 26.** Protect and secure agricultural self-sufficiency in Europe.
- 27.** Secure supply chains for manufactured goods.
- 28.** Develop guidance for the three spaces that identifies potential replacement products and alternative production processes.
- 29.** Promote domestic manufacturing.
- 30.** Support local distribution channels.
- 31.** Increase local recycling rates.

Access to essential services

- 32.** Implement measures that lessen negative consequences and channel cascading failures so that they become more manageable.
- 33.** Regularly assess the vulnerabilities, gaps and needs relating to access to essential services.
- 34.** Evaluate and facilitate the operation of essential services to prevent high impacts and the weaponisation of cascading effects.
- 35.** Ensure that the most vulnerable members of the population can easily and continuously access essential services.
- 36.** Enhance the production capacity of essential services.
- 37.** Identify and diversify, through a result-based approach, innovative ways that guarantee the provision of essential services through various processes.
- 38.** Provide advance communication to the public on how to cope with disruptions to essential services, following the models adopted by several EU MS and partners.

ANNEX 2: COUNTERMEASURES FOR DETERRENCE



1. Public actions with democratic opposition of autocratic adversaries

● STRATEGIC SIGNAL

Description of the countermeasure

Political support for democratic movements, organisations and parties is essential not only to exert pressure on adverse autocratic regimes but also to ensure that democracy ultimately prevails.

Conditions of efficiency

Political action must be grounded in strategic communication that is leading, impactful, disruptive and efficient. Without pushing for any specific electoral output and in full respect of third parties' democratic processes, this approach is, however, crucial for delivering effective messaging about the importance of democracy to both the local population and the international community.

Guiding examples

Using derision regarding attackers, exposing the flaws and absurdities of the regime, and emphasising the legitimacy of democratic leaders to build public trust and support.

2. Documented condemnation of violations of human rights or international law

● LONG-TERM DETERRENT

Description of the countermeasure

Although symbolic, standing officially for democratic principles provides a sense of direction in the chaotic landscape of world politics.

Conditions of efficiency

Condemning actions that violate international law, and having documentation on hybrid threat actors' misbehaviours directed towards dedicated institutions maintaining a record of legal violations.

Guiding examples

Condemning actions that violate international law, documentation directed towards dedicated institutions maintaining a record of legal violations by hybrid threat actors.

3. Strategic fact sharing

● LONG-TERM DETERRENT

Description of the countermeasure

Addressing the citizens of an autocratic regime demonstrates consideration for society beyond its ruling government. It also undermines the artificial idea of a country-to-country conflict weaponised by autocracies to justify their escalation. Fostering a nuanced and inclusive perspective highlights shared values and aspirations, and cooperation across political divides.

Conditions of efficiency

Engaging with local free broadcasters for fact-based communication is advisable, provided that such cooperation is not counterproductive. Collaboration with these broadcasters can amplify the reach and impact of factual messaging, particularly in environments where independent media is scarce.

Guiding examples

Disseminating fact-based information through various channels to reach a broader audience, particularly in environments where traditional media may be restricted or controlled: private media outlets, social media platforms, samizdat or dazibaos.

4. Restrictions on bilateral cooperation

● STRATEGIC SIGNAL

Description of the countermeasure

Public cooperation often persists even in adverse situations, particularly in the economic, social and cultural domains. Restricting such cooperation can be used as a bargaining tool, where limitations are imposed to exert pressure.

Conditions of efficiency

Operating in coordination with partner countries helps to build a united front. Broadly disseminating information about these coordinated efforts and explaining their rationale to both democratic and autocratic societies promote transparency and understanding. This approach underscores the importance of extended deterrence.

Guiding examples

Expelling diplomats at the continental level as a significant diplomatic measure that can be taken in response to severe breaches of international norms or agreements, sending strong signal of disapproval and limiting hostile activities.

5. Collaboration with allies on deterrent initiatives

● STRATEGIC SIGNAL

Description of the countermeasure

Multilateral cooperation significantly enhances the effectiveness of collective decisions by leveraging the combined resources, expertise and influence of participating entities. Additionally, it reinforces the

legitimacy and credibility of the decisions. By fostering shared responsibility and mutual accountability, multilateral cooperation promotes more impactful outcomes while limiting escalation.

Conditions of efficiency

This powerful tool should be implemented as broadly as possible. By engaging a wide range of stakeholders, this approach ensures that collective efforts are well coordinated and widely supported. Additionally, exploring other channels, such as partnerships with international organisations, civil society and the private sector, can further enhance the reach and impact of multilateral initiatives.

Guiding examples

Identifying shared values, fostering convergent interests between Western and non-Western democracies, forging alliances that transcend regional and cultural divides, and enhancing the resilience of democratic institutions.

6. Regulating actions within the framework of common organisations

● LONG-TERM DETERRENT

Description of the countermeasure

Beyond diplomatic efforts such as naming and shaming, the UN and regional organisations offer mechanisms for legal action that can establish and condemn violations of international law. This approach sends a clear message that unchecked behaviour will not be tolerated.

Conditions of efficiency

It is essential to gather allies to support initiatives. This involves building a coalition of like-minded countries and stakeholders that share a commitment to the rule of law. Even if accountability is limited, it is still important to not leave the attacker's reputation intact, to uphold the rule of law and promote adherence to global norms.

Guiding examples

Suspending the adversary's participation in regional and international organisations or ad hoc multilateral cooperation mechanisms, in accordance with their regulations, after the adversary's hybrid threat operations.

7. Action in international justice

● LONG-TERM DETERRENT

Description of the countermeasure

The International Court of Justice (ICJ), the International Criminal Court (ICC), and special tribunals should be empowered to the greatest extent possible to enhance international regulatory frameworks. Strengthening these institutions is a crucial objective in countering the alignment of autocratic regimes.

Conditions of efficiency

To expedite the process, it is essential to enlist the support of various actors, including journalists, open source intelligence (OSINT) practitioners, democratic activists and civil-society organisations, to gather evidence. This collaborative effort should focus on identifying violations of international law and substantiating reports of them.

Guiding examples

Disseminating locally sourced, verified imagery that documents a state's violations of international law, supporting ongoing investigation and supporting the institutions conducting these investigations.

8. Opening of investigations with universal jurisdiction

● RAPID ACTIVATION

Description of the countermeasure

Beyond the cases involving nationals and binational individuals affected by the actions of a hostile country, universal jurisdiction provides a mechanism for judicial action against perpetrators, regardless of their level of responsibility. To be effective, this approach needs robust legal effort focused on qualification and evidence gathering.

Conditions of efficiency

Collaboration with partner democracies on judicial and police matters is essential to implement these decisions.

Guiding examples

Conducting trials for war crimes committed in a non-EU country and issuing arrest warrants that can be enforced by allied nations to further strengthen the pursuit of justice.

9. Intelligence collection strategy aimed at key vulnerabilities

● PROACTIVE MEASURE

Description of the countermeasure

Collecting data on an adversarial regime's weak points enhances bargaining power.

Conditions of efficiency

The coherence of the collection strategy should be ensured among national services and allied services in connection with EU capacities – the European Union Satellite Centre (SatCen), for instance, and the SIAC for analysis – and also economic intelligence and OSINT actors.

Guiding examples

Mapping the economic dependencies and fragile institutional spots of an autocratic regime, in collaboration with like-minded partners.

10. Practising open intelligence

● PROACTIVE MEASURE

Description of the countermeasure

Publishing intelligence collected by national services allows democratic societies to highlight ongoing hybrid threat operations or those in preparation, as early attribution strengthens resilience and preparedness. This can draw on individual Member States' capabilities with their agreement as originator (SIAC / HFC, SatCen, EEAS delegations).

Conditions of efficiency

Founding attribution on solid intelligence, potentially originating from multiple EU MS and partners and cross-checked, is necessary to mitigate the cognitive biases of political decision-makers and the general public and to reinforce trust in society.

Guiding examples

Exposing hybrid threat operations in preparation (cyber, space, information, military defence, etc.), providing

detailed information related to the actors involved; triggering international law mechanisms and political condemnations, and proactive anticipation.

11. Joint Member States domestic and foreign intelligence's countering action

● IMMEDIATE SIGNAL

Description of the countermeasure

A cooperative platform for coordinated EU MS actions against adversarial intelligence services that aim to harm EU interests domestically or internationally could contribute to deterrence.

Conditions of efficiency

Proposals for capabilities should be exchanged among EU MS to enhance the deterrent effect. Political commitment from EU MS through a shared threat assessment and joint action is essential.

Guiding examples

Gathering intelligence from outside Member States through joint operations, reinforcing efforts to disrupt adversarial intelligence networks operating across several EU MS, thwarting hostile intelligence-based operations both within and beyond the EU, and providing strategic signalling and deterrence against future adversarial activities.

12. Collective intelligence collection on economic security

● PROACTIVE MEASURE

Description of the countermeasure

A collective and cooperative approach among Member States' intelligence organisations, both within the territory of the EU and globally, should safeguard shared interests, foster solidarity between EU MS, bolster business development and enhance market penetration.

Conditions of efficiency

Efforts to overcome commercial disputes and competition among EU MS and prioritise cooperation with Member States over extra-EU partners would defend EU strategic interests against external interference. Closely engaging the private sector, anticipating future developments and identifying long-term strategic common interests are prerequisites.

Guiding examples

Coordinating shared responsibilities and budgets in European industrial projects involving diverse EU MS companies, reaching agreements on energy supplies from outside the EU, exporting EU services and goods to third countries and optimising supply chains at the EU level.

13. International counter-espionage investigations with democratic partners

● RAPID ACTIVATION

Description of the countermeasure

Intelligence cooperation between specialised services can be enhanced, particularly in counter-espionage operations, through the deployment of mixed teams that share specific strategies, collection methods, analytical approaches and information and also share common interests and objectives.

Conditions of efficiency

This requires fostering a culture of trust in partnerships for intelligence collection and sharing between EU MS and like-minded partners, strengthening processes and dedicated structures (bilateral, minilateral, multilateral, regional, EU, NATO, EU–NATO) and clearly defining the specificities and conditions of cooperation.

Guiding examples

Neutralising adversarial espionage networks in different EU MS and partner countries.

14. On-demand security meeting of a global alliance of democracies

● STRATEGIC SIGNAL

Description of the countermeasure

Democracies worldwide should develop initiatives, and ideally establish a permanent framework, to coordinate collective actions such as joint public statements, proposals for United Nations General Assembly or Security Council resolutions, and other initiatives at the regional and international levels across various domains. These efforts should aim to counter hybrid threat operations, align economic interests and practices, and defend democracy globally.

Conditions of efficiency

This requires affirming that democracy is not a Western regime and acknowledging the diverse forms of democracy. Strong support should be given to locally rooted and home-grown democratic movements and processes. This can pave the way for an alliance of democracies worldwide on the basis of current alignments. Such an alliance could be open not only to states but also to representatives of democratic movements.

Guiding examples

Gathering security meetings of such a group to address specific hybrid threat operations and reinforce the deterrent leverage of its members.

15. Transnational initiatives with civil societies

● LONG-TERM DETERRENT

Description of the countermeasure

Society-to-society diplomacy can be a valuable asset in establishing connections with countries where regimes attempt to isolate their populations and create antagonism to solidify their grip on power.

Conditions of efficiency

Society-to-society engagement should be treated as an autonomous process by providing diasporas, human rights civil-society organisations and businesses with the necessary financial, technological, infrastructural and geographical means. This support should enable them to foster closer and more constructive contacts, particularly in emerging democracies.

Guiding examples

Enabling local NGOs to financially and logistically support the civil society of a democratic society struggling for its survival, and securing NGOs' databases outside a hostile regime.

16. Democracy-oriented collective defence partnerships

● PROACTIVE MEASURE

Description of the countermeasure

EU-led collective defence initiatives could not only serve as a European pillar of NATO but also, in alignment with the principle of strategic autonomy, establish a democracy-oriented collective defence framework. This framework would encompass democratic states across all continents and condition military partnerships and weapons procurement accordingly.

Conditions of efficiency

Based on the sovereign decisions of Member States, this initiative should be designed to be incentivising and didactic for partner nations, with a preference for the most structural and comprehensive approach. It could be linked to the global alliance of democracies to enhance its effectiveness and reach.

Guiding examples

Improving interoperability, conducting advanced military exercises, and facilitating weapons sales to democratic partner nations.

17. Steps towards reinforcing European defence capabilities

● LONG-TERM DETERRENT

Description of the countermeasure

This measure collectively safeguards Europe, while honouring the sovereign participation of each individual Member State.

Conditions of efficiency

This requires adapting the EU regulatory framework to minimise bureaucratic barriers to military cooperation, including exercises, and enhancing integration at the strategic, operational and tactical levels.

Guiding examples

Increasing the cooperation formats available to combat-capable military units and creating a European Security Council (European Commission, 2026b).

18. Announcements of unified weaponry projects

● STRATEGIC SIGNAL

Description of the countermeasure

This measure consolidates EU MS efforts around unified weapons development in key areas: joint command and control system (C2), unmanned aerial systems (UAS), counter-UAS (C-UAS), unmanned surface vehicles (USV), unmanned ground vehicle (UGV), long-range assets, electronic warfare or logistics capacities.

Conditions of efficiency

This requires engaging with the military industry at the EU level, incentivising projects, facilitating negotiations and decisions, and publicly communicating these efforts collectively to enhance their strategic impact.

Guiding examples

Building common systems of weapons in different locations in Europe.

19. Military procurement and stockpiling initiatives

● PROACTIVE MEASURE

Description of the countermeasure

This measure enhances and sustains constantly developing procurement, the stockpiling of weaponry and ammunition, and medical countermeasures (including but not only CBRN) to ensure long-term combat readiness, thereby contributing to deterrence efforts.

Conditions of efficiency

Efforts should strengthen the defence industry, leverage EU coordination for procurement, establish EU-level stockpiles and develop EUcMS distribution capabilities to ensure the effective sharing of resources.

Guiding examples

Procuring high-tech and low-tech ammunition, including 155 mm strategic ammunition and NATO-standard rifle ammunition. Countering capacities should be treated with agility, as they are subject to quick changes, such as long-range missiles and rockets, as well as ground, surface and aerial unmanned systems.

20. Creation of active reserves

● STRATEGIC SIGNAL

Description of the countermeasure

An active reserve model could potentially serve as a deterrent factor.

Conditions of efficiency

Decision-making at the policy level, cross-cutting implementation at the technical level, regular training and readiness for combat operations are key objectives.

Guiding examples

Improving interoperability collaboration among reserve forces, drills and manoeuvres.

21. Public–private military communication exercises

● STRATEGIC SIGNAL

Description of the countermeasure

Regular reviews, evaluations and adaptations of military communication exercises could be conducted in collaboration with specialised European companies.

Conditions of efficiency

There should be a focus on both high-tech and low-tech solutions, ensuring the compatibility of communication systems and protocols across the continent.

Guiding examples

Testing interoperable, data-sharing battlefield management system (BMS), generating and sharing instructive data to foster innovation.

22. Military logistics studies, programmes and exercises

● LONG-TERM DETERRENT

Description of the countermeasure

Enhancing collective military logistics is essential to signal readiness and ensure preparedness. Military logistics exercises can also serve as a countermeasure to address hybrid threats.

Conditions of efficiency

Increased resources, enhanced capabilities, improved connectivity and more frequent exercises are required.

Guiding examples

Establishing comprehensive connectivity across the entire EU territory for military academies.

23. Bilateral EU agreements with third countries on military supply chains

● STRATEGIC SIGNAL

Description of the countermeasure

Certain materials are essential for conducting cutting-edge research, manufacturing weaponry and waging war, and could be subject to measures to prevent hostilities.

Conditions of efficiency

Cooperating on access to resources (military, economic), making decisions at the EU level and receiving support from diplomatic and business sectors are essential.

Guiding examples

Imposing sanctions or blockades to restrict adversaries' access to supply chains for critical raw materials.

24. EU military drills

● STRATEGIC SIGNAL

Description of the countermeasure

This involves conducting joint military exercises to enhance deterrence, interoperability, preparedness and readiness. These drills can incorporate varying levels of intensity to align with projected scenarios.

Conditions of efficiency

This requires focusing on real-world threats and incorporating various domains, including electronic warfare and cyberdefence.

Guiding examples

Integrating military exercises with real deployment scenarios to enhance the deterrent effect.

25. Partial or full mobilisation of reservists

● STRATEGIC SIGNAL

Description of the countermeasure

The mobilisation of reservists can be both planned and executed as a means of signalling intent and enhancing preparedness.

Conditions of efficiency

This requires basing the mobilisation on concrete intelligence-driven anticipation rather than escalation fears, coordinating with other EU MS and integrating with territorial defence measures.

Guiding examples

Preventing military tension at an external EU border by sending a strategic signal.

26. Tripwire force deployment in Member States and partner countries

● STRATEGIC SIGNAL

Description of the countermeasure

As already implemented, a limited tripwire force can have a deterrent effect by signalling to the adversary that any intervention might entail unwanted consequences. This approach can be applied across land, sea, air and space military domains.

Conditions of efficiency

This requires widely communicating the situation and associated political demands to ensure visibility and legitimacy, while engaging as many partners as possible. The potential strategic and operational implications should be carefully considered in the decision-making process.

Guiding examples

Implementing multinational air defence missions in a Member State or an allied country facing military aggression, such as Ukraine in Russia's war of aggression.

27. Response readiness signal

● STRATEGIC SIGNAL

Description of the countermeasure

Any preparation, deployment or act of intimidation should be met with clear and decisive signals of readiness.

Conditions of efficiency

Decisive political resolve, strategic solidarity, and the availability and readiness of necessary resources are essential.

Guiding examples

Implementing air, sea and land defence missions, enhancing military patrolling and establishing a permanent military presence in strategic locations.

28. Operating the EU Rapid Deployment Capacity in anticipation

● PROACTIVE MEASURE

Description of the countermeasure

The deployment of this force should follow a high state of alert from Member States.

Conditions of efficiency

Enhancing the scale of involved capabilities, accelerating deployment speed, streamlining deployment processes as much as feasible, and ensuring that military mobility infrastructure is both prepared and safeguarded.

Guiding examples

Applying the EU RDC to hybrid kinetic operations, encompassing but not limited to military activities.

29. Automatic destruction of hostile unmanned military vehicles

● IMMEDIATE SIGNAL

Description of the countermeasure

Where the local population is not placed in greater jeopardy, consideration may be given to the destruction of unmanned military vehicles, even if these vehicles are destined for a third country.

Conditions of efficiency

The political resolve and collective defence spirit are crucial. It is imperative not to allow any instance of illegal transgression or dangerous threats of destabilisation and destruction to go unanswered.

Guiding examples

Applying this measure not only to unmanned aerial vehicles (UAVs) but also to UGVs, USVs and to unmanned underwater vehicles (UUVs) and implementing it to both autonomous and remotely operated vehicles.

30. Indicating common resolve against violations of Member States' territory or assets

● IMMEDIATE SIGNAL

Description of the countermeasure

This involves the justified enforcement of national and international law in cases of violations of airspace, sea space or land space by a hostile state using military or civilian means, by a range of possible measures, including immobilisation, seizure or destruction, as indicated by the circumstances and in applicable laws.

Conditions of efficiency

The absence of decisive action encourages and invites hostile actors to repeat and escalate their transgressions. Clear strategic signalling of a refusal to tolerate such actions can demonstrate resolve in defending all dimensions of the territory and protecting political sovereignty. This approach should be pursued as much as possible in collaboration with allies to reinforce the strategic impact.

Guiding examples

Ordering the intervention of naval capabilities, the arrest of foreign personnel and the seizure of the vessel. Uncooperative violations of airspace could result in the destruction of the aircraft. Instances of land territory violations may lead to the arrest or destruction of the intruding forces.

31. Launch of territorial defence preparation

● PROACTIVE MEASURE

Description of the countermeasure

Consideration could be given to developing plans for civilian territorial defence battalions. These units would be activated in the early stages of military escalation, enhancing both deterrence and readiness.

Conditions of efficiency

This requires adapting to the EU MS' systems regarding conscription and reserves, with these units being framed and commanded by regular military forces. Implementing strict weaponry control, providing financial incentives for equipment acquisition and integrating the measure into escalation management are also essential.

Guiding examples

Training land forces in pre-conflict situations to increase deterrence.

32. Strategic communication campaign emphasising the disparities in development

● STRATEGIC SIGNAL

Description of the countermeasure

The levels of economic development and opportunities significantly differ between democracies and most autocracies. This fact could be used during a targeted strategic communication campaign.

Conditions of efficiency

Such a campaign should be locally tailored, target a specific objective, directly engage the population, be supported by concrete examples of developmental disparities and connect these differences to the regime's hostility and inefficiency.

Guiding examples

Highlighting the stark living conditions in comparison with those in democracies in an online campaign.

33. Sanctions against regime's officials, descending to lower administrative levels

● STRATEGIC SIGNAL

Description of the countermeasure

As it already exists, this countermeasure could be extended to include lower levels of the public administration, particularly but not only those in security, defence and economy.

Conditions of efficiency

It is important to clearly and widely communicate the rationale behind the sanctions and specify the conditions for their potential reversal.

Guiding examples

Implementing positive and negative incentives for members of military or non-state armed groups.

34. Sovereign bonds and currency release

● RAPID ACTIVATION

Description of the countermeasure

Sovereign bonds and currency reserves, once released strategically, could disrupt the economy.

Conditions of efficiency

This requires safeguarding against retaliation and coordinating with partners to strengthen the impact.

Guiding examples

Introducing a large amount of the adversary's currency into the market to disrupt its macroeconomic policies.

35. Severing commercial ties

● RAPID ACTIVATION

Description of the countermeasure

Significant reductions in business presence not only disrupt cooperation but also deprive the population of high-quality goods.

Conditions of efficiency

Making decisive and collective decisions, preventing diversion through other countries and ensuring the effects in terms of trade disruption are essential.

Guiding examples

Severing ties in the natural resources market or that of manufactured goods.

36. Secondary sanctions against third countries with significant cooperation with adversaries

● STRATEGIC SIGNAL

Description of the countermeasure

Countries, companies or individuals with close ties with adversaries may be subjected to secondary sanctions, as already used in certain cases.

Conditions of efficiency

This requires utilising cross-cutting cooperation to enhance the lever effect, implementing both negative and positive incentives for third countries and taking measured actions to prevent partners from being pushed towards alliances with autocratic countries.

Guiding examples

Preventing business exchanges involving dual-use civil–military goods.

37. Surveillance, control and custody of assets used to conduct hybrid threat operations

● IMMEDIATE SIGNAL

Description of the countermeasure

Based on solid intelligence or evidence, all assets used to conduct operations should be immobilised to prevent recurrence, evasion and denial. They should remain under strict control and surveillance until justice investigations are concluded.

Conditions of efficiency

This tool should be used with strong resolve to resist diplomatic pressure, including from third parties – such as private companies or states – that may be voluntarily or involuntarily involved in the operation. It should also be as automatic as feasible and supported by allies to produce a deterrent effect.

Guiding examples

Immobilising financial (funds, accounts), material (transportation, facilities, intelligence-gathering means, weapons) or human (foreign or domestic) assets. All assets should be considered. The case of diplomatic staff is particularly sensitive regarding international law but should be strictly addressed.

38. Seizure of assets used to conduct hybrid threat operations

● IMMEDIATE SIGNAL

Description of the countermeasure

Material assets that are proved to have been voluntarily used to conduct hybrid threat operations could be seized by the victim state.

Conditions of efficiency

Although some attacks might not be significantly impactful due to the involvement of immaterial or low-cost assets, others might be when costly assets are involved. The legal basis for such a countermeasure could be framed, for example, by the 2001 UN International Law Commission (ILC) Articles on the Responsibility of States for Internationally Wrongful Acts (ARISWA), adopted by the UN General Assembly in 2002 (United Nations General Assembly, 2002). Although it is not a binding treaty, it can be considered international customary law. It defines the conditions for a state to be held responsible for breaking international law.

Guiding examples

Seizing maritime transport ships, air assets or any material assets utilised to conduct hybrid threats operations.

39. International containment of space technologies

● LONG-TERM DETERRENT

Description of the countermeasure

Preventing access to technologies is a way to at least limit the expansion of the space domain, particularly through space-dedicated economic actors.

Conditions of efficiency

This requires cooperating with the private space sector, preventing direct investments in autocratic regimes' space programmes and advocating for regulations to address the use of space for hybrid threat operations.

Guiding examples

Preventing adversaries from developing their space capacities, such as obtaining satellite launchers.

40. Sanctions against institutions and companies involved in hybrid threat operations

● RAPID ACTIVATION

Description of the countermeasure

Strategic institutions and sanctioned companies could be legally or technically blocked in response to hybrid threat operations.

Conditions of efficiency

This requires publicly communicating the cyber response to an attack suffered by a Member State, leveraging actions through cross-cutting cooperation at the technical level, with the aim of achieving a deterrent effect in the future.

Guiding examples

Potentially blocking governmental services and digital platforms, at least in the targeted country.

41. Detection using applications and software of military personnel operating in the grey zone

● IMMEDIATE SIGNAL

Description of the countermeasure

OSINT can enable the collection of valuable information on the movement of military troops, as demonstrated in Syria and Ukraine.

Conditions of efficiency

The civic space, including investigative journalism and OSINT entities, and the services space, such as software developers, can prove to be of great value to the governance space, encompassing intelligence, analysis and decision-making.

Guiding examples

Detecting the presence of soldiers, who frequently use standard applications and social media platforms during their deployments.

42. AI-powered enhancer to improve open democratic content on social media

● RAPID ACTIVATION

Description of the countermeasure

The use of AI is widespread among autocratic regimes and groups for conducting cognitive warfare. It can also be employed to disseminate pro-democracy messaging.

Conditions of efficiency

To maintain the democratic nature of the tool, the message should transparently disclose that it was created by AI and utilise levers other than fear or hate, such as interest or humour.

Guiding examples

Disseminating effective messages based on a nuanced understanding of the population.

43. Impactful fines if social media do not cut AI promoting autocratic or highly polarising messaging

● RAPID ACTIVATION

Description of the countermeasure

Very large online platforms (VLOPs) and very large online search engines (VLOSEs) may be inclined to permit activities linked to hybrid threat operations from autocracies to be conducted on their platforms. The governance space must be clear and decisive in establishing boundaries regarding the threats it is willing to accept through these platforms.

Conditions of efficiency

Regulation, along with positive and negative incentives for operators, can effectively limit the spread of subversive campaigns on social media, search engines and private messaging systems.

Guiding examples

Fining VLOPs and VLOSEs in breach of regulation compliance to preserve democracy, as it is the prerogative of the governance space to regulate the services space.

44. Online advertising on social media about the benefits of democracies

● STRATEGIC SIGNAL

Description of the countermeasure

Citizens from autocratic regimes may have a strong affinity for democratic countries, which can be reinforced and spread.

Conditions of efficiency

Highlighting the connection, within democratic societies, between fundamental rights and cultural, social and economic development can positively leverage the appeal of the country.

Guiding examples

Incorporating cultural symbols, personalised language references, hobbies and travel-related content to enhance the effectiveness of messaging.

45. Scaled fact-based operation on language models

● LONG-TERM DETERRENT

Description of the countermeasure

Countering autocratic data poisoning can protect democracy and support factual content to influence adversarial AI machine learning models.

Conditions of efficiency

Shorter elements are preferable to longer ones, as they are more challenging for AI to detect.

Guiding examples

Implementing counter-influence strategies against autocratic regimes by drawing inspiration from the regimes' own practices, adapted to defend and promote democratic values.

46. Signalling AI-trained anti-missile and anti-drone systems deployed

● STRATEGIC SIGNAL

Description of the countermeasure

In alignment with the development of a European drone wall and the Eastern Flank Watch, signalling the deployment of countering systems can have a deterrent effect.

Conditions of efficiency

The performance of countering systems varies, and their deployment should be carefully calibrated to ensure a substantial impact on the adversary's intentions.

Guiding examples

Implementing countermeasures in a multilayer distribution at the border.

47. Deployment of an AI tool against disinformation in a contested environment

● LONG-TERM DETERRENT

Description of the countermeasure

While not foolproof, certain AI tools can serve as a shield against disinformation in specific contexts.

Conditions of efficiency

It could be a software or hardware solution. However, given the potential for traceability, it may not be feasible to operate in highly controlled areas.

Guiding examples

Deploying AI tools in regions with high levels of foreign information manipulation and interference (FIMI) or during times of crisis.

48. Collective protective cyber operations

● IMMEDIATE SIGNALL

Description of the countermeasure

Cybersecurity is essential for the normal functioning of a democratic society. During periods of heightened tensions, these operations can be conducted in collaboration with services and civic spaces.

Conditions of efficiency

This tool would require individuals to possess robust IT skills, although dedicated training could also be provided, for example within the framework of national reserve programmes or specialised courses.

Guiding examples

Using civilian IT software, hardware and networks, in addition to the involvement of personnel not involved in security and defence, to improve capacities.

49. Targeted campaigns of transparency

● STRATEGIC SIGNAL

Description of the countermeasure

Special information platforms could be established to disseminate key pieces of information, particularly regarding social rights, economic performance and issues of corruption and nepotism.

Conditions of efficiency

This requires integrating every operation within a strategic communication framework and openly providing all necessary information.

Guiding examples

Demonstrating how poor economic decisions have resulted in severe social consequences.

50. Journalism media consortia

● LONG-TERM DETERRENT

Description of the countermeasure

Collaborations between EU media outlets and exiled independent media can make it possible to conduct investigations, leveraging the sources of the latter and the distribution networks of the former.

Conditions of efficiency

No institutional involvement is required beyond establishing a legal framework and providing incentives for EU media to initiate these consortia.

Guiding examples

Facilitating and supporting free journalism through the provision of resources and assistance.

51. Collaborative network of national psychological defence agencies ⁽⁸⁾

● STRATEGIC SIGNAL

Description of the countermeasure

A network of institutions dedicated to societal resilience and security could have a significant deterrent effect.

⁽⁸⁾ A rationale for this measure has been established by the Warsaw Security Forum (Warsaw Security Forum, 2025).

Conditions of efficiency

Collaboration among agencies is crucial to foster robust solidarity among allies, notwithstanding the unique characteristics of their societies.

Guiding examples

Establishing an information network, the exchange of best practices, practical exercises, simulations and guidance to strengthen each participating society.

52. Twinning of NGOs

● STRATEGIC SIGNAL

Description of the countermeasure

An EU-based NGO could partner with an autocracy-based NGO, providing support either within the regime or in exile.

Conditions of efficiency

This requires no direct institutional involvement, ensuring decisional and operational autonomy for the local NGO, with reciprocal exchanges based on the principle of equality.

Guiding examples

Offering material and legal assistance to a local NGO engaged in human rights advocacy.

53. Regular collective addresses by decision-makers on the state of democracy in the world

● STRATEGIC SIGNAL

Description of the countermeasure

Regular addresses from democratic decision-makers to citizens living under autocratic regimes could help dismantle propagandist narratives against democracy.

Conditions of efficiency

This requires promoting the message that citizens' voices matter and that liberal democracy is founded on freedom, which can be done through internet- and event-based campaigns tailored to specific countries.

Guiding examples

Proceeding to regular communication campaigns about the development of democracy in the world, highlighting how democracies derive their policy decisions from the will of their citizens.

54. 'Culture versus politics' initiative

● LONG-TERM DETERRENT

Description of the countermeasure

Cultural initiatives aimed at societies can counter the notion that democracies criticise autocracies for reasons other than the hostile and oppressive nature of the regimes.

Conditions of efficiency

This requires supporting and promoting local artists who are critical of the autocratic regime through events, broadcasts and publications.

Guiding examples

Organising concerts featuring pro-democracy artists from autocratic regimes.

55. Culture-free democracy promotion

● LONG-TERM DETERRENT

Description of the countermeasure

Internet platforms can demonstrate that democracy can be embraced regardless of cultural background, showcasing various forms of democratic systems without consideration of culture, in order to break adversarial attempts to 'Westernise' democracy and prevent non-Western societies from realising their democratic aspirations.

Conditions of efficiency

This requires emphasising the inherent connection between local political culture and democracy by drawing on historical examples of the struggle for representativeness.

Guiding examples

Creating platforms broadcasting images of peaceful demonstrations, didactic presentations of human rights, interviews and testimonies.

56. Periodic strategic review of cultural cooperation

● LONG-TERM DETERRENT

Description of the countermeasure

To prevent the politicisation of culture by authoritarian regimes, a regular review should assess the strategic relevance of maintaining bilateral cooperation in this domain if culture is weaponised to glorify the regime.

Conditions of efficiency

Recognising that culture is politicised and weaponised by autocracies, an objective review of cooperation should be conducted with the assistance of independent experts, ensuring the entire process is transparent and public.

Guiding examples

Cutting cultural cooperation ties with a country that exploits its culture to legitimise its autocratic regime.

57. Preventing the weaponisation of culture to advance hostile foreign interests

● STRATEGIC SIGNAL

Description of the countermeasure

If cultural personalities position themselves or are empowered as political representatives supporting the

autocracy's narrative, they may be barred by the Member State from performing in the EU, as they could be considered agents of influence promoting the autocracy's political agenda within the EU.

Conditions of efficiency

This requires a transparent and educational decision grounded in appropriate legal measures, openly communicating the rationale and the risks of allowing sedition and subversion to use culture as a vector.

Guiding examples

Making the internet available in a border region where a democratic movement is subject to a ban by an autocratic regime. Several approaches can be considered: overriding MAC addresses on laptops, end-to-end encryption (E2E), peer-to-peer encrypted communication through additional encrypted systems (P2P-E), and providing free access to online VPNs with hidden connections.

Getting in touch with the EU

In person

All over the European Union there are hundreds of Europe Direct centres. You can find the address of the centre nearest you online (european-union.europa.eu/contact-eu/meet-us_en).

On the phone or in writing

Europe Direct is a service that answers your questions about the European Union. You can contact this service:

- by freephone: 00 800 6 7 8 9 10 11 (certain operators may charge for these calls),
- at the following standard number: +32 22999696,
- via the following form: european-union.europa.eu/contact-eu/write-us_en.

Finding information about the EU

Online

Information about the European Union in all the official languages of the EU is available on the Europa website (europa.eu).

EU publications

You can view or order EU publications at op.europa.eu/en/publications. Multiple copies of free publications can be obtained by contacting Europe Direct or your local documentation centre (european-union.europa.eu/contact-eu/write-us_en).

EU law and related documents

For access to legal information from the EU, including all EU law since 1951 in all the official language versions, go to EUR-Lex (eur-lex.europa.eu).

Open data from the EU

The portal data.europa.eu provides access to open datasets from the EU institutions, bodies and agencies. These can be downloaded and reused for free, for both commercial and non-commercial purposes. The portal also provides access to a wealth of datasets from European countries.

Science for policy

The Joint Research Centre (JRC) provides independent, evidence-based knowledge and science, supporting EU policies to positively impact society



Scan the QR code to visit:

The Joint Research Centre

<https://joint-research-centre.ec.europa.eu>



**Publications Office
of the European Union**

Law | Data | Publications