European Commission

Joint Research Centre

Defending Europe Against Hybrid Warfare

EXECUTIVE SUMMARY

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

JRC 148340
EUR 40871

Print ISBN 978-92-68-44033-9 ISSN 1018-5593 doi:10.2760/4528358 KJ-01-26-428-EN-C
PDF ISBN 978-92-68-44032-2 ISSN 1831-9424 doi:10.2760/0222094 KJ-01-26-428-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. For any use or reproduction of photos or other material that is not owned by the European Union permission must be sought directly from the copyright holders.

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 - Executive summary*, Publications Office of the European Union, Luxembourg, 2026, https://data.europa.eu/doi/10.2760/0222094, JRC148340.

Defending Europe Against Hybrid Warfare

EXECUTIVE SUMMARY

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

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.

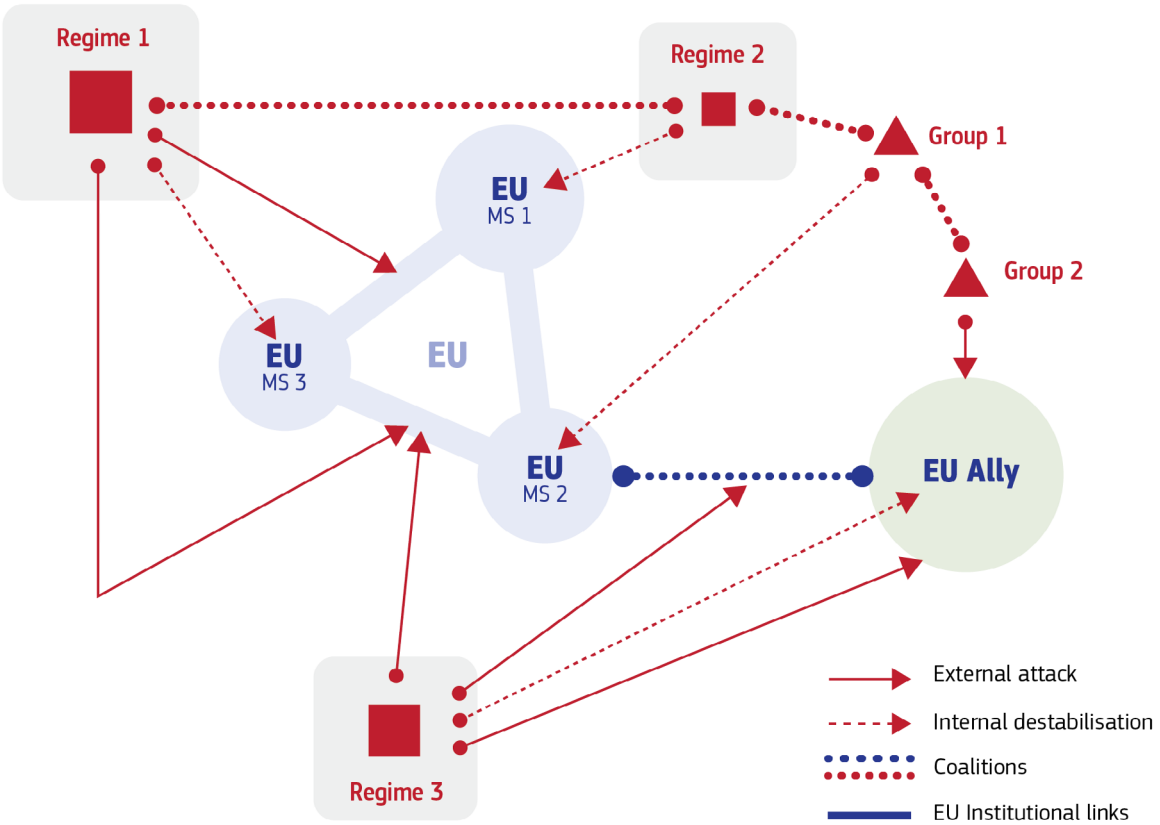
They exploit the linearity of escalation theory, using deception and surprise to create key disruptions. While signals still exist, HIOs demand a reinforced cognitive ability to anticipate and analyse attacks properly. They might be kinetic attacks as well as attacks of an immaterial nature. Designed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

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 or internal destabilisation. 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.

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 by 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.

FIGURE 1

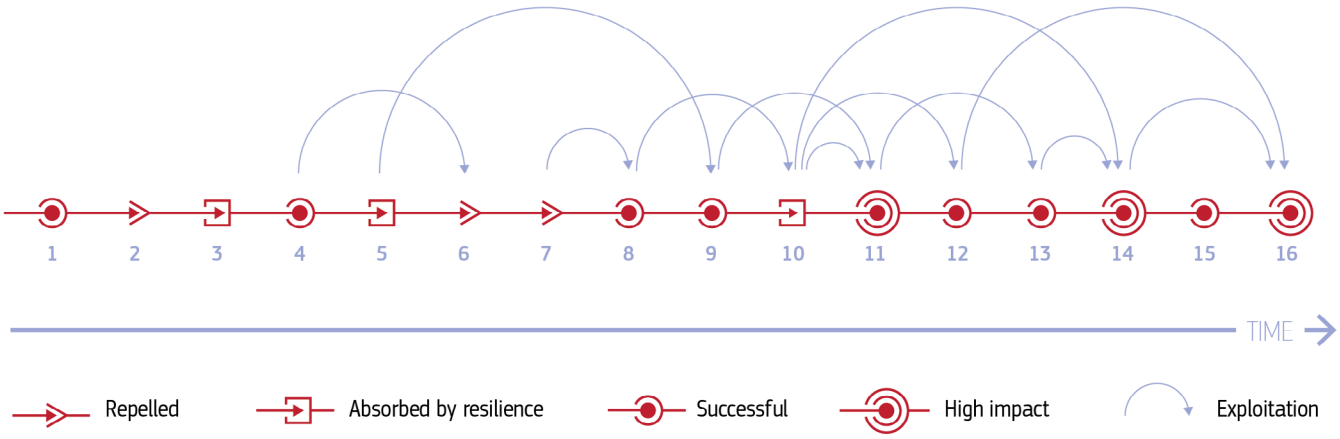
Multi-actor saturation of European security ecosystem[2]



Source: EU

FIGURE 2

Multiple exploitation of cascading effects



Source: EU

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.

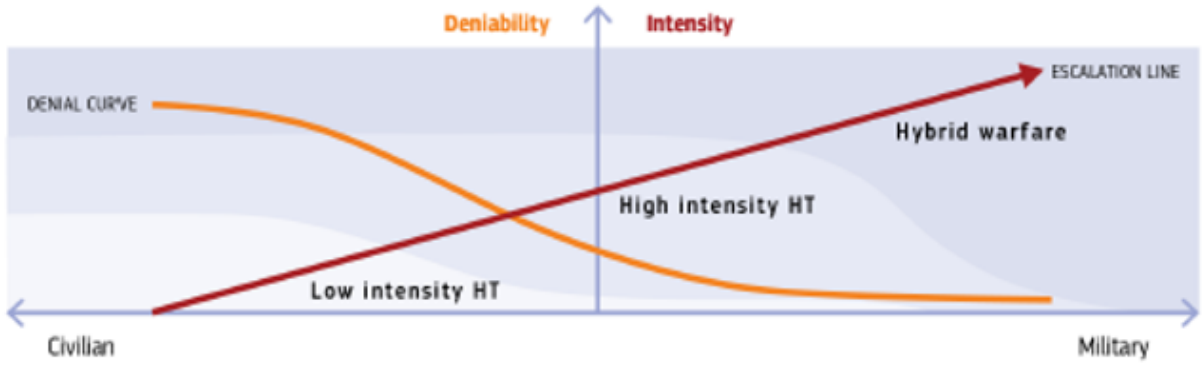
On the policy side, the concept of hybrid warfare has been endorsed. EU MS government and state officials use the concepts of 'hybrid warfare' or 'hybrid war' to qualify the situation.

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"[1].

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

FIGURE 3

Hybrid threat operations' escalation to hybrid warfare



Source: EU

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.

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.

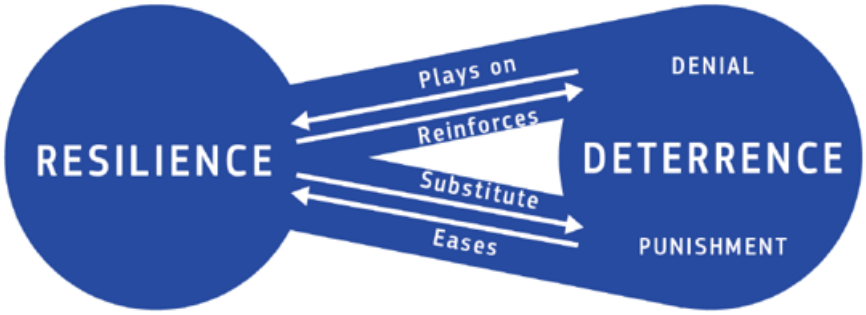
Deterrence and resilience must be closely coordinated from a very early stage at the strategic level. The success of a tailored security strategy depends on this upstream strategic coordination.

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

FIGURE 4

Proactive anticipation



Source: EU

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.

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.

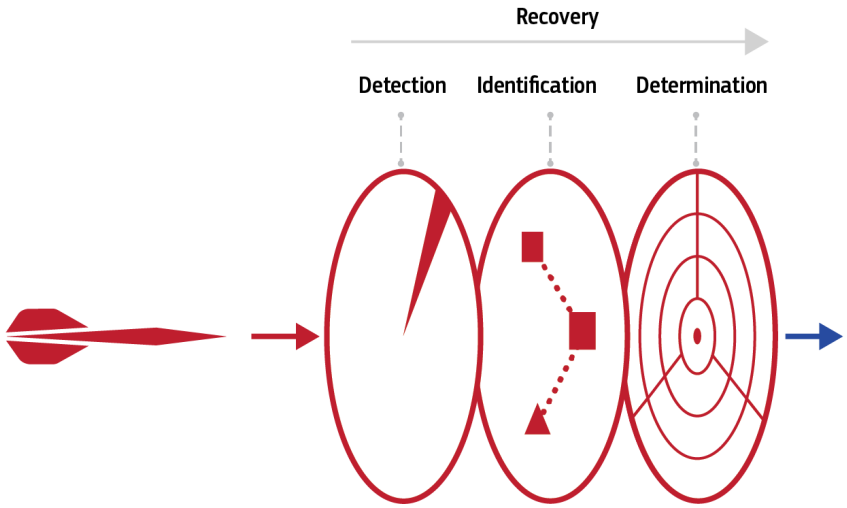
The two additional elements are essential and have specific characteristics.

- **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.

FIGURE 5

Active defence



Source: EU

3. Reactive retaliation

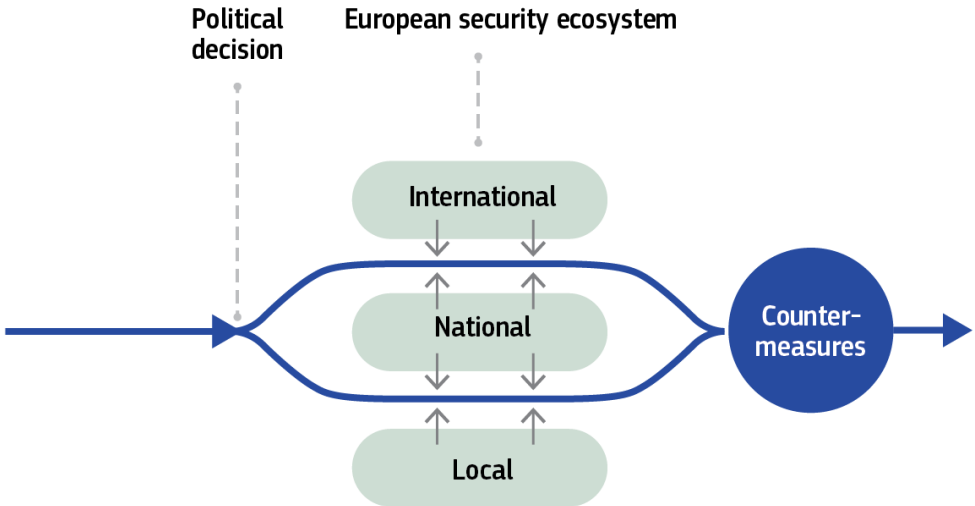
To prevent an escalation in intensity and to avoid a slide into more severe conflicts, a response strategy should amplify the adversary's costs through deterrence. Europe must therefore act swiftly to increase cost imposition within the grey zone by deploying countermeasures. Reactive response follows 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.

FIGURE 6

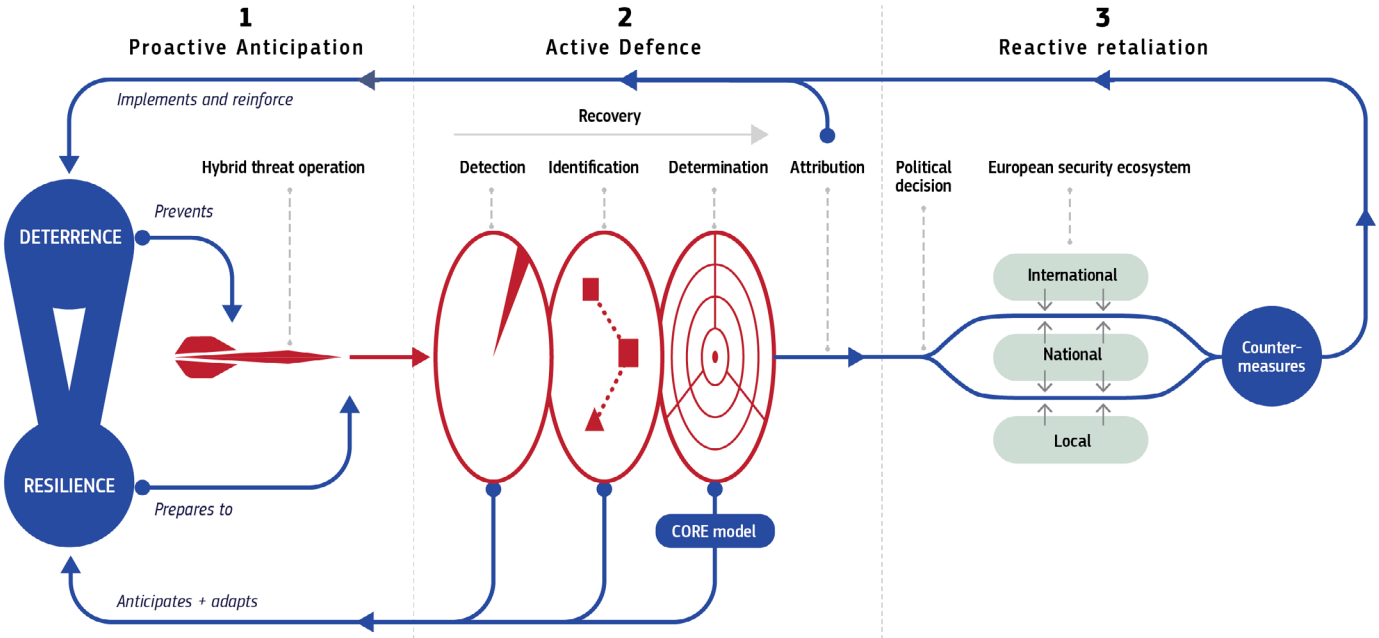
Reactive retaliation



Source: EU

FIGURE 7

Resilience-deterrence strategy



Source: EU

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.
- Reputational accumulation – Repeated attributions and the visible imposition of costs cause reputational damage to the adversary.

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