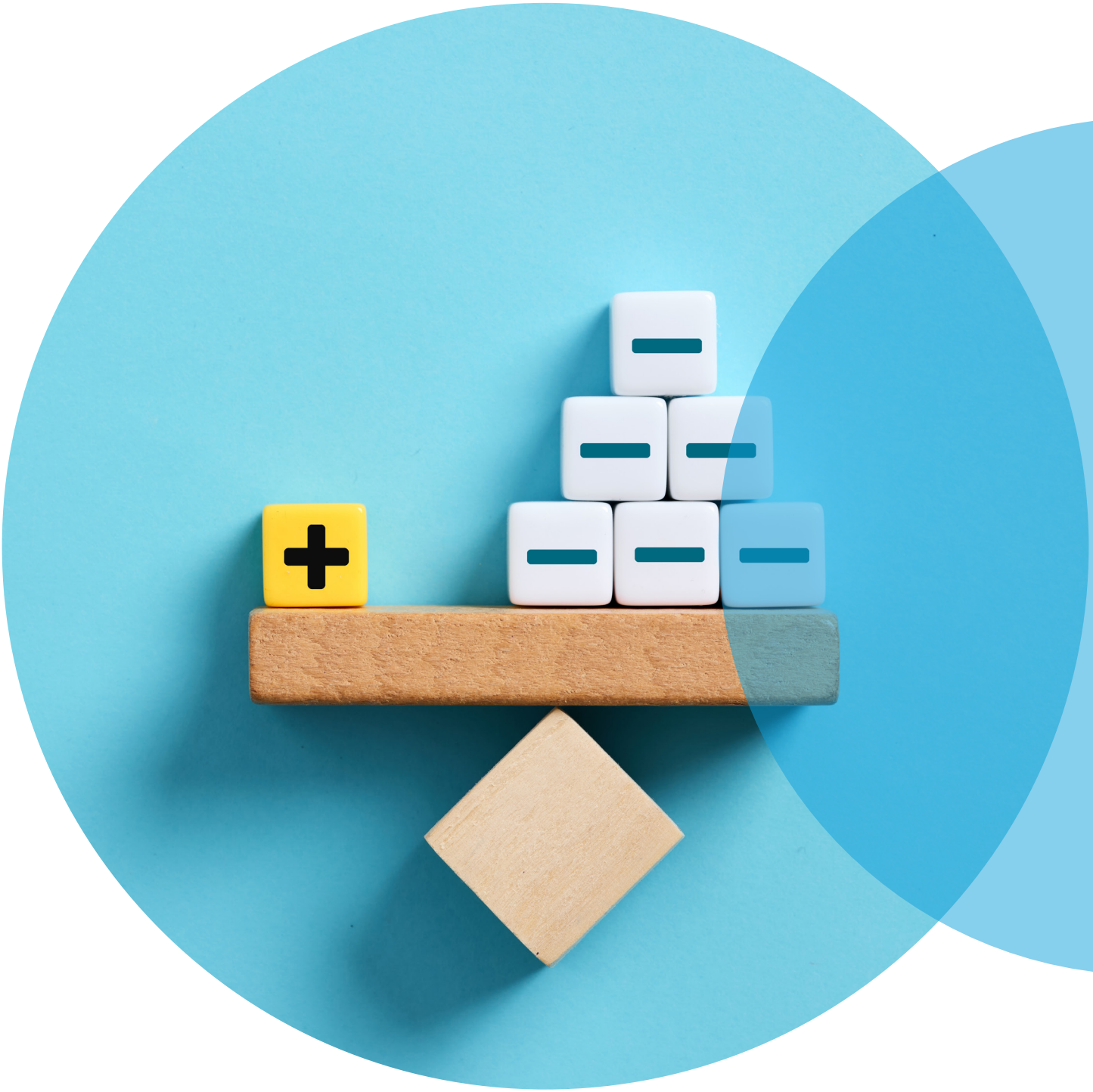
Hybrid CoE Paper 25

# Turning strategy into praxis: Lessons in hybrid threat deterrence



Hybrid CoE

Viktorija Rusinaitė – August 2025

**Hybrid CoE Papers** are finalized pieces of analysis on a topic related to hybrid threats, based on one or several research questions. They may be either conceptual analyses or based on a concrete case study with empirical data.

---

**The European Centre of Excellence for Countering Hybrid Threats**
tel. +358 400 253800 www.hybridcoe.fi

ISBN 978–952–7591–24–6 (web)
ISBN 978–952–7591–25–3 (print)
ISSN 2670–2053 (web)
ISSN 2814–7227 (print)

August 2025

Cover photo: Cagkan Sayin / Shutterstock.com

**Hybrid CoE's mission** is to strengthen its Participating States' security by providing expertise and training for countering hybrid threats, and by enhancing EU-NATO cooperation in this respect. The Centre is an autonomous hub for practitioners and experts, located in Helsinki, Finland.

# Contents

# Summary

This paper explores how conventional deterrence theory and practice are being adapted to counter hybrid threats, proposing three ways to maximize the efficiency of this process. First, it examines the critical impact of a whole-of-government approach, and the ability of practitioners from different institutions to collaborate on strategies. Second, the paper looks into the pitfalls of entanglement as an alternative strategy to deterrence. While this can be counterproductive if applied to large, aggressive adversaries, it is more promising with norm-adherent adversaries. Third, the paper proposes the balanced use of cost imposition and benefit denial, combined with increased cultural awareness. The paper shows that insufficient cultural understanding of the adversary leads to distorted situational awareness and detrimental approaches, such as avoiding escalation at all costs. Drawing on observations and analyses gleaned from deterrence tabletop exercises conducted by Hybrid CoE between 2020 and 2023, the paper presents these findings as three key lessons learned.

# Introduction

The enhanced connectivity of modern societies creates new vulnerabilities as the hybrid threat landscape continues to expand. Hybrid threat actors can use social networks to gain convenient and direct access to populations. From banking to shipping, everything is plugged into an information network. Artificial intelligence makes disruption more efficient and cost-effective. Hybrid threat actors also have more opportunities to obstruct systems, while these same systems help them to obscure identification, delay attribution, and hinder the implementation of countermeasures.

The evolving threat landscape requires a rethinking of deterrence, even if its fundamental principles remain unchanged. While the nuclear umbrella and military strength might deter a conventional military attack, today's hybrid threat actors seek to disrupt the societal, governmental and infrastructural processes[1] that enable societies to resist foreign interference and defend themselves now and in the future.

Against this backdrop, this paper briefly discusses hybrid threat deterrence theory and practice, drawing on lessons learned from tabletop exercises conducted within the framework of Hybrid CoE's deterrence programme.

**Lesson 1: *The one-room transformation*** emphasizes how an integrated approach is needed to transform deterrence. It suggests that *if practitioners from different ministries and agencies do not meet and work together, it will be detrimental to their deterrence strategies.* These strategies depend on who is in the room, the capabilities they possess, their thresholds for action, and their motivation to coordinate with other actors.

**Lesson 2: *The pitfalls of entanglement*** demonstrates that entanglement, or the creation of mutual dependencies to sustain peace, is challenging with large, aggressive adversaries, but may yield results with norm-adherent or smaller ones.

**Lesson 3: *The trouble with escalation avoidance*** shows how illusions of shared norm frameworks impede deterrence, and how the value of peace expressed through escalation avoidance leads to an exaggerated focus on resilience.

The aim of the paper is to provide policy practitioners with experience-based insights into enhancing the deterrence of hybrid threats in light of these challenges. The findings are based on observations collected throughout the 2021–2023 deterrence programme conducted at Hybrid CoE.[2]

1 Georgios Giannopoulos et al., 'The Landscape of Hybrid Threats: A Conceptual Model', (Publications Office of the European Union, February 2021), https://www.hybridcoe.fi/publications/the-landscape-of-hybrid-threats-a-conceptual-model/.

2 During this time, over 200 practitioners were trained, and 7 national and multinational educational tabletop exercises were conducted.

# Deterrence of hybrid threats in theory: Squaring the circle

This paper and Hybrid CoE's broader approach to deterrence[3] borrow notions from classical deterrence, such as cost-benefit calculus,[4] direct and extended deterrence, escalation, and thresholds, adapting them to the landscape of hybrid threats.[5] By expanding the threat landscape beyond traditional military threats, this body of work departs from classical deterrence thinking, or what is often referred to as the narrow concept of deterrence.[6] This traditional thinking is rooted in nuclear and conventional military capabilities, the resolve to retaliate if necessary (in other words, credibility), as well as communication activities to ensure that the adversary is aware of both resolve and credibility. Alongside exploring the adaptation of these three pillars to the landscape of hybrid threats, this chapter also introduces multidomain and actor-specific approaches to deterrence.

This classical understanding of deterrence is built on three pillars: communication, capability and resolve. In principle, it works in the following way: for deterrence to function, a signal must be communicated to the adversary that the capabilities to overpower them exist and will be used against them if necessary.[7] While there is general scholarly agreement that these pillars are relevant to conventional deterrence, they require adjustment when applied to the complexity of hybrid threats.

Although the number of tanks, nuclear warheads and capabilities is quantifiable, and national resolve is outlined to some extent in security and similar strategies, matters become murkier when it comes to deterring hybrid threats. The capability to deliver small blows across a range of non-military and military domains to achieve a cumulative effect on the adversary on the one hand, and the ability to provide and receive credible extended deterrence through alliances, unions

3 Vytautas Keršanskas, 'Deterrence: Proposing a More Strategic Approach to Countering Hybrid Threats', (Hybrid CoE, March 2020), https://www.hybridcoe.fi/publications/hybrid-coe-paper-2-deterrence-proposing-a-more-strategic-approach-to-countering-hybrid-threats/.

4 Michael J. Mazar, 'Understanding Deterrence', (RAND Corporation, April 2018), https://www.rand.org/pubs/perspectives/PE295.html.

5 Keršanskas, 'Deterrence: Proposing a More Strategic Approach to Countering Hybrid Threats'.

6 Sean Monaghan, Hybrid CoE Paper 12: 'Deterring Hybrid Threats: Towards a Fifth Wave of Deterrence Theory and Practice', (Hybrid CoE, March 2022), 21–22, https://www.hybridcoe.fi/publications/hybrid-coe-paper-12-deterring-hybrid-threats-towards-a-fifth-wave-of-deterrence-theory-and-practice/.

7 In US deterrence theory, the categories of resolve, capability, and communication can be traced back to the classics. On resolve, see: Thomas C. Schelling, 'The Art of Commitment', in *Arms and Influence* (New Haven and London: Yale University Press, 2020), 35–91, https://doi.org/10.12987/9780300253481–005. On capabilities and resolve, see: Robert Jervis, 'Chapter Three. Deterrence, the Spiral Model, and Intentions of the Adversary', in *Perception and Misperception in International Politics* (Princeton University Press, 2017), 58–114, https://doi.org/10.1515/9781400885114–006. On communication and signalling – in addition to resolve and capabilities – see: Monaghan, Hybrid CoE Paper 12: 'Deterring Hybrid Threats: Towards a Fifth Wave of Deterrence Theory and Practice'.

and partnerships on the other, are both much more complex to evaluate.[8] For example, the EU's resolve to impose economic sanctions can be undermined by the opposition of a single member state. Similarly, NATO's resolve requires consensus. In 2001, when the 9/11 terror attacks occurred in the US, Article 5 of the North Atlantic Treaty was intended solely for cases of armed military attack.[9] To invoke Article 5 in response to the 9/11 attacks, NATO officials argued that commercial planes had been used by the terrorists as missiles to hit the buildings, and that the event could therefore be regarded as an armed attack.[10] The Allies accepted this argument, and Article 5 was invoked for the first time in response to a terrorist operation. This precedent illustrates NATO's ability to adapt quickly to different situations. This was further reinforced by the 2022 Strategic Compass, which states that "Hybrid operations against Allies could reach the level of armed attack and could lead the North Atlantic Council to invoke Article 5 of the North Atlantic Treaty".[11] Nevertheless, consensus among all Allies would still be required to recognize a specific attack as qualifying for the triggering of Article 5. Hence, it allows hostile actors to conclude that NATO's resolve can be impeded by the opposition of a single member state.

Moreover, the capabilities to deter a foreign state from establishing corruption networks and exerting economic influence depend on the efforts of the police, public administration, security services, and even investigative journalists. However, these capabilities are not usually communicated to a hostile actor as part of a security strategy, meaning that their mere existence does not necessarily deter hybrid threat actors.

These examples demonstrate how challenging it is to adapt the pillars of communication, capability and resolve for the purpose of deterring hybrid threats. Within Hybrid CoE's deterrence framework, particular attention has been paid to the ways in which hybrid threats erode these three pillars. Such threats undermine the communication of deterrence because they rely on ambiguity to avoid attribution. Without clarity about who needs to be deterred, communication to the target audience also becomes unclear. Hybrid threats also erode capability as they use novel, cross-domain means to generate cumulative effects against which military tools are ineffective. Finally, hybrid threats undermine the credibility of deterrence. While individual activities may appear insignificant in terms of

8 For example, Rupal N. Mehta argues that extended deterrence provided by the US can be characterized by uncertainty, even in traditional security environments. Concerns over credibility may increase with the use of cross-domain capabilities, such as cyber, space, and others. Rupal N. Mehta, 'Extended Deterrence and Assurance in Multiple Domains', in *Cross-Domain Deterrence: Strategy in an Era of Complexity*, ed. Eric Gartzke and Jon R. Lindsay (Oxford University Press, 2019), https://doi.org/10.1093/oso/9780190908645.003.0011.

9 NATO, 'The North Atlantic Treaty', 4 April, 1949, https://www.nato.int/cps/en/natohq/official_texts_17120.htm.

10 NATO Review, 'NATO Review – Invoking Article 5', 1 June, 2006, https://www.nato.int/docu/review/articles/2006/06/01/invoking-article-5/index.html.

11 'NATO 2022 – Strategic Concept', 29 June, 2022, https://www.nato.int/strategic-concept/.

engaging the state machinery and deterrence, their cumulative effect might be powerful.[12]

To support the conventional pillars of deterrence against erosion by hybrid threats, Hybrid CoE has identified three key elements: agility, solidarity and attribution. Agility enables rapid mobilization across government sectors, while solidarity is required to provide a collective response through the EU and NATO. Finally, without attribution, it is difficult to launch response measures tailored to a specific actor.[13]

The key takeaway is that the deterrence of hybrid threats calls for an adjustment to the classical theory of deterrence to reflect these new realities. As hybrid threats are characterized by the coordinated and synchronized use of a wide range of means to exploit systemic vulnerabilities, influence decision-making and undermine targets, with actors seeking to remain below the thresholds of detection and attribution,[14] deterrence theory must adapt accordingly.

As hostile actors target vulnerabilities across a range of domains, the deterrence of hybrid threats requires a **multidomain**, **cumulative**, **and actor-specific approach**. Anticipation, risk planning, and both response and prevention can also originate in multiple domains.

Rather than aiming to prevent hybrid threat activities from occurring, this approach investigates how to shrink the space available for adversaries to carry them out. The realistic approach explored in this paper is **cumulative and restrictive** in nature, rather than based on absolute deterrence.[15]

Deterring hybrid threats requires an actor-specific approach.[16] Identifying the hostile actor when developing a deterrence strategy helps prioritize where to build resilience, and how to tailor responses to impact the actor in a meaningful way. The aim is to make an attack less attractive by shifting the hostile actor's cost-benefit calculus in such a way that the risks associated with the attack outweigh the expected benefits. This is easier to achieve when one is able to identify the hostile actor and its characteristics, values, interests, and vulnerabilities, all of which need to be at the heart of the deterrence posture.

While deterrence against hybrid threats can rarely prevent hostile campaigns altogether, its goal is to restrict the attack perimeter and therefore minimize the effect. Rather than focusing on the military perspective, the deterrence of hybrid threats addresses a range of attacks against both civil and military domains that could disrupt the functioning of society. In such cases, preventative deterrence is rarely an option because it is difficult to anticipate and respond in advance to activities occurring in multiple domains. Of course, individual attacks, such as those against payment systems, can be prevented by

12 Monaghan, Hybrid CoE Paper 12: 'Deterring Hybrid Threats: Towards a Fifth Wave of Deterrence Theory and Practice'.
13 Keršanskas, 'Deterrence: Proposing a More Strategic Approach to Countering Hybrid Threats'.
14 Hybrid CoE – The European Centre of Excellence for Countering Hybrid Threats, 'Hybrid Threats as a Concept', accessed 18 June 2025, https://www.hybridcoe.fi/hybrid-threats-as-a-phenomenon/.
15 Monaghan, Hybrid CoE Paper 12: 'Deterring Hybrid Threats: Towards a Fifth Wave of Deterrence Theory and Practice'.
16 Keršanskas, 'Deterrence: Proposing a More Strategic Approach to Countering Hybrid Threats'.

higher-level cyber protections,[17] and the activities of known disinformation actors can be curtailed using legal instruments.[18] However, this will not prevent entire campaigns; rather, resilience and the imposition of costs will make it more difficult to implement their various components.

17 Anne Kauranen, 'Exclusive: Nordics and Estonia Rolling out Offline Card Payment Back-up in Case Internet Cut', *Reuters, 7 May, 2025*, https://www.reuters.com/business/finance/nordics-estonia-plan-offline-card-payment-back-up-if-internet-cut-2025-05-07/.

18 Vytautas Keršanskas, Hybrid CoE Paper 6: 'Deterring Disinformation? Lessons from Lithuania's Countermeasures since 2014', April 2020, https://www.hybridcoe.fi/publications/deterring-disinformation-lessons-from-lithuanias-countermeasures-since-2014/.

# Lesson 1. The one-room transformation: Strategies based on a whole-of-government approach

State systems are divided into domains, with ministries and agencies responsible for implementing government decisions within specific legal frameworks. Hybrid threat actors deliberately exploit vulnerabilities that fall between these domains and often produce effects across several of them. For instance, rather than targeting a specific ministry of a given country, adversaries are more likely to focus on vulnerabilities that cut across ministerial silos. Thinking across domains is therefore essential to any coherent strategy for deterring hybrid threats. This requires both an integrated whole-of-government and a broader whole-of-society approach.[19] However, findings from Hybrid CoE's deterrence programme show that such coordination rarely occurs in advance of a crisis. In order to change this, an integrated approach to transforming hybrid threat deterrence is needed. This section looks into the main considerations required for a whole-of-government approach to work as intended.

**State agencies and institutions collectively have a wide range of tools at their disposal** to create a comprehensive deterrent effect. Each organization typically has a clear grasp of its own mandate and operates with a specific set of tools. However, synchronizing these tools and their effects is not possible without effective coordination. For example, political attribution[20] could be aligned with sanctions that diminish the adversary's ability to perpetrate further hybrid attacks. Achieving this requires intelligence on how the adversary is carrying out such threats. Military or preparedness exercises can then be planned along with targeted communication campaigns aimed at citizens, allies, and the adversary's elites. This, in turn, calls for the involvement of institutions such as the Ministry of Foreign Affairs, the Ministry of the Economy, intelligence agencies, the Ministry of Defence, the military, and the Ministry of the Interior.

In terms of its mechanics, the deterrence of hybrid threats involves the imposition of costs and the denial of benefits in order to reduce the hostile actor's room for manoeuvre. The imposition of costs entails demonstrating to the adversary – through the threat of punitive measures – that the perceived benefits of an attack will be outweighed by its detrimental consequences. Denial means preventing the adversary from achieving the intended benefits of the attack. The simplest way to do this is often by increasing the resilience of the relevant domain(s), rendering the hostile actor's activities futile.[21]

19 See Rainer Jungwirth et al., 'Hybrid Threats: A Comprehensive Resilience Ecosystem' (Publications Office of the European Union, March 2023), https://www.hybridcoe.fi/wp-content/uploads/2023/04/CORE_comprehensive_resilience_ecosystem.pdf, 83. See also Dick Zandee et al., 'Countering Hybrid Threats', (Clingendael, October 2021), https://www.clingendael.org/pub/2021/countering-hybrid-threats/, and Mikael Wigell et al., 'Best Practices in the Whole-of-Society Approach in Countering Hybrid Threats', (European Parliament, May 2021), https://www.europarl.europa.eu/thinktank/en/document/EXPO_STU(2021)653632.

20 Different forms of attribution exist and are relevant to the deterrence of hybrid threats. Among these, the most relevant are: technical attribution – based on the traces left by a proxy of a hostile actor (relevant in cyber and some disinformation campaigns); legal attribution – evidence-based attribution through judicial systems and courts; and political attribution – conducted by political leaders, parliamentary groups and so on, using political instruments such as statements, reports, etc.

21 Keršanskas, 'Deterrence: Proposing a More Strategic Approach to Countering Hybrid Threats'.

**Many of the tools required to build resilience to hybrid threats will lie outside traditional security-oriented departments** – namely, outside the Ministries of the Interior, Foreign Affairs, and Defence. However, representatives not affiliated with these ministries typically do not view their roles as contributing to deterrence. For example, responsibility for both short- and long-term societal resilience would fall somewhere between the Ministry of Culture, the Ministry of Education, the Ministry of Social Affairs and Health, and the Ministry of Defence. Ministries that are not oriented towards security may also have **different perspectives on risk and cost-benefit calculations**. This is why it is important to include them in discussions on hybrid threat deterrence, rather than simply issuing directives. For example, restricting exports of dual-use technologies might not be viewed positively by the Ministry of the Economy, where the general objective is often to promote trade. Without effective coordination, it becomes difficult to reconcile differing perspectives on thresholds for deterrent action.

Traditional security-oriented organizations tend to lean towards punishment due to their focus on crisis management and safety. If practitioners are **managing one crisis after another, they will have no time for resilience building**; instead, they will be predisposed to imposing costs on the perpetrator. As a result, systems resort to sanctions, such as expelling a hostile actor from international organizations or engaging in coercive diplomacy. When deterrence strategies are not designed to incorporate economic, educational, cultural or legal capabilities, they often lack complexity and focus only on short-term solutions.

**When experts from different institutions meet in one room to communicate and resolve problems more efficiently, they can arrive at more innovative and comprehensive solutions.** In the absence of such collaboration, however, estimates of how long certain actions will take can vary widely between ministries. For example, outside the Ministry of Defence, other ministries and agencies may estimate that acquiring a weapons system takes a couple of months, when in fact it might take years. Similarly, understanding the mechanics of a strategic communications campaign helps all actors plan goals, timelines, and desired effects more realistically.

Overall, open communication channels between different state institutions significantly improve the efficiency of deterrence-related problem-solving. Each institution can offer a valuable and distinct perspective on the threat, along with a range of possible solutions. In a group setting, experts can reach a more nuanced understanding of the nature of hybrid threats and ways to counter them. By considering all available capabilities, their combined impact, and realistic timelines, the final strategy stands a better chance of being targeted, pragmatic, and ultimately successful.

# Lesson 2. The pitfalls of entanglement: Do not invite a fox into the henhouse

Entanglement[22] is an alternative strategy to deterrence, which **aims to create a situation in which an adversary, by choosing to attack, would inadvertently harm its own interests in the process**.[23] Such an approach emphasizes a continuous relationship between adversaries based on mutual dependencies. These dependencies may include economic interests such as import and export relationships, logistics routes, infrastructure projects (including roads, railways and ports), and technology transfers, as well as partnership agreements. By pursuing common goals and interests, and by establishing partnerships, countries simultaneously create dependencies. Whereas deterrence is based on a cost-benefit analysis and operates through denial and cost imposition,[24] entanglement focuses on creating meaningful mutual benefits, thereby creating a disincentive for aggressive behaviour.[25]

Based on the findings of Hybrid CoE's tabletop exercises, two main practical challenges emerge in applying the entanglement approach to hybrid threats: managing aggressive adversaries and addressing the mismatch in size and capability between actors. While the entanglement strategy may appear on paper to offer more room for manoeuvre and to prevent losses, it is a challenging approach in practice, requiring good timing and an in-depth understanding of the adversary and its motivations. To entangle a state amid an adversarial relationship, concessions must be made and rewards – or so-called "carrots" – must be provided, while punishments – or "sticks" – must be withheld. Careful consideration, resourcefulness, and restraint are therefore required.

**If an adversary is perceived as aggressive, the inclination is not to try to forge mutual dependencies, but rather to break free from existing dependencies to avoid further losses**. As one participant in a tabletop exercise put it: *"You do not try to entangle a fox in a henhouse. It will eat the chickens!"* When dealing with an aggressive adversary, there is a danger that concessions and rewards offered as part of an entanglement strategy may be seen as a sign of weakness, emboldening the adversary to engage in more aggressive behaviour rather than encouraging compliance.[26] Furthermore, efforts to forge partnerships with adversaries

22 In some sources, entanglement is referred to as inducement. See e.g., Colin Gray, *Maintaining Effective Deterrence* (Carlisle, PA: Strategic Studies Institute, US Army War College, 2003), 15.

23 Tim Sweijs and Samuel Zilincik, 'The Essence of Cross-Domain Deterrence', in *NL ARMS Netherlands Annual Review of Military Studies 2020: Deterrence in the 21st Century—Insights from Theory and Practice*, ed. Frans Osinga and Tim Sweijs (T.M.C. Asser Press, December 2020), https://doi.org/10.1007/978-94-6265-419-8_8, 129–58.

24 The definition of deterrence in terms of deterrence by imposition of costs and deterrence by denial is often traced back to Glenn H. Snyder. See e.g., Glenn H. Snyder, 'Deterrence and Power', *The Journal of Conflict Resolution 4*, no. 2 (1960): 163–78.

25 Aaron Brantly, 'Conceptualizing Cyber Deterrence by Entanglement' (David L Boren College of International Studies, March 2018), http://www.ou.edu/cis/research/cyber-governance-and-policy-center/the-cyber-governance-blog/conceptualizing-cyber-deterrence-by-entanglement.html.

26 Stephen Van Evera, 'The Spiral Model vs. the Deterrence Model', in *II34 Hypotheses on the Causes of War*, (MIT OpenCourseWare, 1997), https://web.mit.edu/17.423/www/Archive98/handouts/spiral.html. See also: Robert Jervis, 'Chapter Three. Deterrence, the Spiral Model, and Intentions of the Adversary', in *Perception and Misperception in International Politics* (Princeton University Press, 2017), https://doi.org/10.1515/9781400885114-006, 58–114.

that adhere to different sets of norms are likely to be unpredictable. A prime example of the failure to entangle an actor with a different value set involved Germany's efforts to solidify mutual dependencies with Russia via a trade relationship, including energy supplies.[27] These mutual dependencies failed to deter Russia's aggressive behaviour, including the annexation of Crimea, the assassination of Chechen field commander Zelimkhan Khangoshvili on German soil, and Russia's full-scale invasion of Ukraine. Moreover, these dependencies created conditions that encouraged Russia to intensify its malign activities by influencing public discourse through disinformation and Russia-friendly actors in order to maintain the cash flow. Once this was no longer possible, Russia sought to blackmail Germany by cutting gas supplies to prevent the imposition of sanctions.

Another major obstacle to entanglement is that **individual states in Europe are smaller and weaker than their adversaries**. Their arsenals and militaries are typically more limited than those of their more heavily militarized opponents. Larger and more "thuggish" adversaries are more likely to see inducements as concessions to their threats and military might, interpreting efforts to establish mutual connections and dependencies as weakness rather than goodwill. As a result, entanglement might provoke further aggression and thuggish behaviour.[28] To amplify their influence, individual European states consistently rely on multilateral alliances such as NATO and the EU,[29] which form a key part of their strategies for deterring larger, more aggressive adversaries. NATO's military toolbox, and the economic policy and diplomatic tools of the EU provide small states with leverage against hostile actors that they would not otherwise possess.

The size-capability mismatch, different values, and aggressiveness all help to explain the current deterrence-based punishment-centred approach towards Russia, which is perceived as a large, norm-defiant hostile actor. However, what about the entanglement of smaller states, or hostile intermediaries and allies? These are often weaker state or non-state actors that are rarely on a par with stronger deterring states. Depending on the timing of the conflict and their motivations, they could be successfully entangled, giving deterring states more room for manoeuvre. However, based on Hybrid CoE's findings, smaller states, proxies and intermediaries are often overlooked. One reason for this is the lack **of coordination outside a state's non-standard security competences, for example at an economic or legal level. Without these competences, states are unable to design more sophisticated long-term strategies** that could provide incentives and thus create entanglement. This reinforces the first lesson: a diverse set of experts across state institutions must work together to develop a sophisticated strategy that encompasses entanglement.

To recap, deterrence by entanglement is likely to backfire when applied to larger, aggressive, and norm-defying adversaries. However, it may prove more effective with smaller states or intermediaries. Nevertheless, the successful implementation of entanglement strategies requires the involvement of non-traditional security competences in the process.

27 Jungwirth et al., 'Hybrid threats: a comprehensive resilience ecosystem'.
28 Ibid.
29 Keršanskas, 'Deterrence: Proposing a More Strategic Approach to Countering Hybrid Threats'.

# Lesson 3. The trouble with escalation avoidance: Be aware of your biases

In practice, a strategy often plays out differently from how it is laid out on paper. It is implemented through human interactions, within existing institutions that function within the context of both their own and their adversary's strategic cultures. In Western democracies, strategic cultures are distinctively shaped by norms and values that lead to escalation avoidance.[30] These norms and values influence what is deemed acceptable or unacceptable, the willingness to take risks, as well as the capacity to call out what is perceived as unacceptable behaviour. This section expounds on two challenges related to norms and deterrence: a non-escalatory focus on resilience, and mirror imaging. Both challenges demonstrate how differing worldviews between adversaries can result in misinterpretations of what actually deters.

Democracies value peace – at least between each other.[31] One of the norms that supports this value is escalation avoidance. A convenient way to avoid escalation when countering hybrid threats is to focus extensively on resilience.[32] Resilience activities help societies to "withstand stress and recover, strengthened".[33] The concept of resilience applies across all domains and at the multilateral level as well. Activities such as building cross-governmental teams, designing anticipation and defence strategies, or developing information-sharing formats are all important aspects of resilience. Such activities often contribute to long-term solutions and form the main pillars of societal cohesion, strengthening critical infrastructures and services, shortening government response times, and improving administrative and legal preparedness.

Focusing solely on resilience to counter hybrid threats represents an inward-looking approach to deterrence, in which practitioners enhance their own systems, the resilience of the population, and their partnerships. There are unequivocal merits to such internal

30 Peter Dickinson, 'Western Fear of Escalation Will Hand Putin an Historic Victory in Ukraine', (Atlantic Council, April 2024), https://www.atlanticcouncil.org/blogs/ukrainealert/western-fear-of-escalation-will-hand-putin-an-historic-victory-in-ukraine/, and New Europe Center, 'The Failure of "Escalation Management" How Western Fears about Russia Only Deepen and Extend War', 12 December, 2024, https://neweurope.org.ua/en/analytics/proval-menedzhmentu-eskalatsiyi-yak-strahy-zahodu-shhodo-rosiyi-lyshe-poglyblyuyut-ta-rozshyryuyut-vijnu/.

31 Democratic peace theory flourished in the 1980s and 1990s, with the main proponents claiming that democracies are unlikely to go to war with each other and are by nature more peaceful than autocracies. See e.g., Bruce Russett et al., 'The Democratic Peace', *International Security* 19, no. 4 (1995), https://doi.org/10.2307/2539124, 164–84. Dean Babst, 'Elective Governments – A force for peace', *The Wisconsin Sociologist* 3, (1964): 9–14.

32 For example, the main EU documents on hybrid threats overwhelmingly focus on resilience, and the word resilience is referred to extensively throughout the documents, whereas "imposition of costs" or "punishment" either do not appear at all or are mentioned only once. See JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL, 'Joint Framework on countering hybrid threats – a European Union response', (2016), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52016JC0018, or A STRATEGIC COMPASS FOR SECURITY AND DEFENCE | EEAS, 24 March, 2022, https://www.eeas.europa.eu/eeas/strategic-compass-security-and-defence-0_en.

33 JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL, 'Joint Framework on countering hybrid threats – a European Union response'.

improvements: better preparedness means that in an environment where cyber systems, civil contingency plans and media literacy are strengthened, it is more difficult for an adversary to achieve destabilization goals. However, an inward focus fails to communicate to the adversary that the state is unwilling to give in to threats and is prepared to push back. This absence of a threat of punitive measures or any active response further encourages hybrid threat actors to challenge international norms, rules and laws.

Norms provide a platform for commonality and predictability. However, some states view US and European norm-setting as a Western tool of dominance and resist it. **By setting norms for what is and is not acceptable, democracies not only enhance the predictability of the strategic environment but also limit their own room for manoeuvre with regard to their adversaries.** This is extensively exploited by authoritarian adversaries, who challenge international rules and laws and engage in illicit or criminal activities to gain a strategic advantage over democracies, which are unable to use such tools.

Often, adversaries are not only able to perpetrate illicit activities, but also to cast a veil of plausible deniability over their actions. This strategic avoidance of attribution not only helps them to evade the consequences of an attack, but also makes it easier for liberal democracies to cling to the illusion that the adversary thinks like them and adheres to the same norm systems. This misperception of the adversary's nature is called "mirror imaging".[34] Mirror imaging, or assuming that the adversary is similar to us, obscures their goals and methods and leads to flawed deterrence strategies. As Keith B. Payne has noted: "Assuming an opponent to be reasonable according to familiar standards will not provide a reliable basis for anticipating the outcome of deterrence."[35]

Norms, values, and accepted forms of behaviour shape our approaches to hybrid threat deterrence. In particular, escalation avoidance, aimed at maintaining peace, leads to an extensive focus on resilience in order to refrain from confrontation with adversaries. While shared norms provide a sense of predictability among allies, this approach may prove counterproductive with aggressive and militarized adversaries who, like bullies, are likely to be emboldened by targets that avoid confrontation. Moreover, by focusing primarily on resilience, states unnecessarily restrict their ability to deploy the full range of cost imposition tools. Subscribing to the same values might create norms and predictability, but it also requires democracies to uphold them, which naturally restricts their options. Furthermore, assuming that everyone subscribes to the same values can lead democracies to fail to anticipate attacks, while autocratic adversaries exploit the situation under the cover of plausible deniability. Effective strategies to circumvent these pitfalls include involving experts who understand the adversary's norms and ways of thinking during the planning process. Tabletop exercises in which planners imitate an adversary's actions or build strategies from the adversarial perspective can also help to identify and eradicate bias.

34 Keith Payne, *The Fallacies of Cold War Deterrence and a New Direction*. 1st edition (University Press of Kentucky, 2001), 21.

35 Ibid., 92.

# Conclusions

One way to close the norm gap is to maximize the effectiveness of one's approach to deterrence. This paper proposed three ways to do so. First, whole-of-government coordination should be implemented: practitioners should come together to jointly design a deterrence strategy for hybrid threats. Such an approach is essential for developing multidimensional and cohesive strategies. Involving a diverse set of capability owners will ensure that the strategies are aligned with the threat environment, and that a broad range of tools from various domains are used to build resilience and impose costs.

Second, entanglement as a strategy to counter hybrid threats may sound good on paper, but it requires favourable conditions. Large adversaries may perceive attempts at entanglement as a sign of weakness, which is likely to embolden further aggression. Successful entanglement therefore requires a sound understanding of the adversary. It can be deployed to engage smaller, norm-adherent adversaries, proxies, and intermediaries, who may be deterred from hostile behaviour. When entanglement is appropriate, a whole-of-government approach can help to build a more sophisticated strategy, as capability owners from different ministries and agencies can contribute more targeted information about existing bilateral and multilateral cooperation formats with the state in question, the needs of both states in a given domain, and efficient venues for cooperation.

Third, balanced strategies should include both resilience-building and cost-imposition tools, and should be designed with an awareness of "mirror imaging" – the tendency to project one's own value set onto the adversary. Mirror imaging leads to an array of problems, including inadequate situational awareness and a poor understanding of how the adversary might respond to deterrence activities.

A good deterrence strategy will also consider the cultural environment, including norms and values. Adherence to common norms creates a predictable security environment among states. Setbacks occur when those designing deterrence strategies ignore cultural norms and assume that the strategic environment is characterized by a shared 'common sense'.

Furthermore, democratic states might seek to focus solely on resilience and avoid imposing punishment out of fear of escalation. This narrow interpretation of escalation can be self-limiting. Avoiding escalation not only restricts the available options for denial and the imposition of costs, but also overlooks the unique nature of the adversary and how it perceives deterrent actions. If the adversary is strong and hostile and does not subscribe to the same democratic values, it is likely to interpret passive resilience-based approaches as a sign of weakness, which may encourage further aggression.

# Acknowledgements

The author would like express heartfelt appreciation to Stuart Mackie, who led the Community of Interest on Hybrid Influence from 2020 to 2023, co-led the deterrence tabletop exercises, and significantly contributed to the author's understanding of the deterrence of hybrid threats through collaboration, insights and reflections. The author is also deeply grateful to Michael Rademaker, Johan Koers, Irina Patrahau, Björn de Heer, Veera Kaarela, Paul Dickson, Vytautas Keršanskas and many others who, in one way or another, supported and enriched Hybrid CoE's deterrence work from 2020 to 2023.

# Author

**Dr Viktorija Rusinaitė** is Director of the Research and Analysis Function at Hybrid CoE, where she leads a team dedicated to studying threat actors, developing concepts, and conducting comparative analyses of policy solutions. The team serves as a vital bridge between policy practitioners and academic researchers investigating hybrid threats. Prior to her current role, Dr Rusinaitė headed the *Deterrence of Hybrid Threats* project at Hybrid CoE, which focused on innovating classical deterrence approaches and enhancing strategic skills. Before joining Hybrid CoE, she served as Head of the European Security Programme at the Vilnius Institute for Policy Analysis in Lithuania, where her work primarily addressed disinformation and threats posed by both state and non-state actors. Dr Rusinaitė holds a PhD in Political Science from Vytautas Magnus University and is an Eisenhower Fellow.

Hybrid CoE

The European Centre of Excellence
for Countering Hybrid Threats