The Hague Centre
for Strategic Studies

Ten Guidelines for Dealing with Hybrid Threats

A Policy Response Framework

Mattia Bertolini, Raffaele Minicozzi and Tim Sweijs

April 2023

The Hague Centre
for Strategic Studies

Ten Guidelines for Dealing with Hybrid Threats

A Policy Response Framework

Authors:
Mattia Bertolini, Raffaele Minicozzi and Tim Sweijs

April 2023

The research for and production of this report has been conducted within the PROGRESS research framework agreement. Responsibility for the contents and for the opinions expressed, rests solely with the authors and does not constitute, nor should be construed as, an endorsement by the Netherlands Ministries of Foreign Affairs and Defense.

Table of Contents

Executive Summary

Rival states increasingly use hybrid tactics to influence democratic processes and exploit the vulnerabilities of their opponents.

Rival states increasingly use hybrid tactics to influence democratic processes and exploit the vulnerabilities of their opponents. These tactics include the coordinated and synchronised use of violent and non-violent instruments of power to execute cross-domain activities below the threshold of conventional armed military conflict, often circumventing detection and attribution. Fast-paced technological developments and deep global connectedness have provided these states with startling tools to do so. In recent years, Western governments have progressively enhanced their situational awareness and developed capabilities to minimise damages from hybrid threats. In addition, they have also started to respond proactively to hybrid threats by implementing a range of policies to not just increase resilience and bolster defence but also to shape the adversary's behaviour through deterrence measures. Deterrence is broadly defined as discouraging an opponent from taking unwanted actions, which is achieved by persuading an adversary that potential costs outweigh potential gains. Deterrence by punishment implies the threat of severe penalties in response to a potential attack and aims to influence the opponent's strategic calculus by demonstrating that aggressive behaviour has grave consequences. Deterrence by denial, instead, seeks to deny opponents the ability to successfully execute attacks by making it unlikely to succeed.

Conceptual innovation to address hybrid threats has expanded traditional understandings of deterrence and led to the identification of new success factors for deterrence. First, it is recognised that different hybrid threats such as disinformation and cyber operations may not be deterrable in absolute terms. This has led to the refinement of resilience strategies to encompass *strategic denial*, understood as denying not the immediate effect of the action but the political benefits that could be attained from it. Second, deterrence by punishment has come to encompass *deterrence through norms*, *delegitimisation*, and *entanglement* to meet new cross-domain challenges emerging in the grey zone. Deterrence through norms seeks to affect the cost calculus of those that challenge certain standards of behaviour. Delegitimisation, closely aligned to the existence of norms, is a form of punishment through naming and shaming and stigmatisation. Finally, deterrence through entanglement leverages cross-domain interdependencies between states. The core assumption here is that entangled actors will refrain from launching attacks because they will incur costs.

These innovations notwithstanding, deterring hybrid aggressors remains difficult for a variety of reasons. First, hybrid adversaries deliberately circumvent detection and escape responsibility. Second, there are no clear shared rules that regulate acceptable behaviour. Third, defenders lack either the capability or the willingness to respond. Fourth, defenders lack a proper understanding of both the incentive structure and weak spots of rival actors and are consequently unable to design tailored and effective policies that hit the opponent where it hurts. Moreover, defenders are not able to convincingly communicate counter-hybrid policies beforehand. Fifth, the design and execution of counter-hybrid policies often come with potential second- and third-order effects that are not always immediately clear, and a robust understanding of their escalatory dynamics is lacking. This in turn serves as an impediment for defenders to execute counter-hybrid responses.

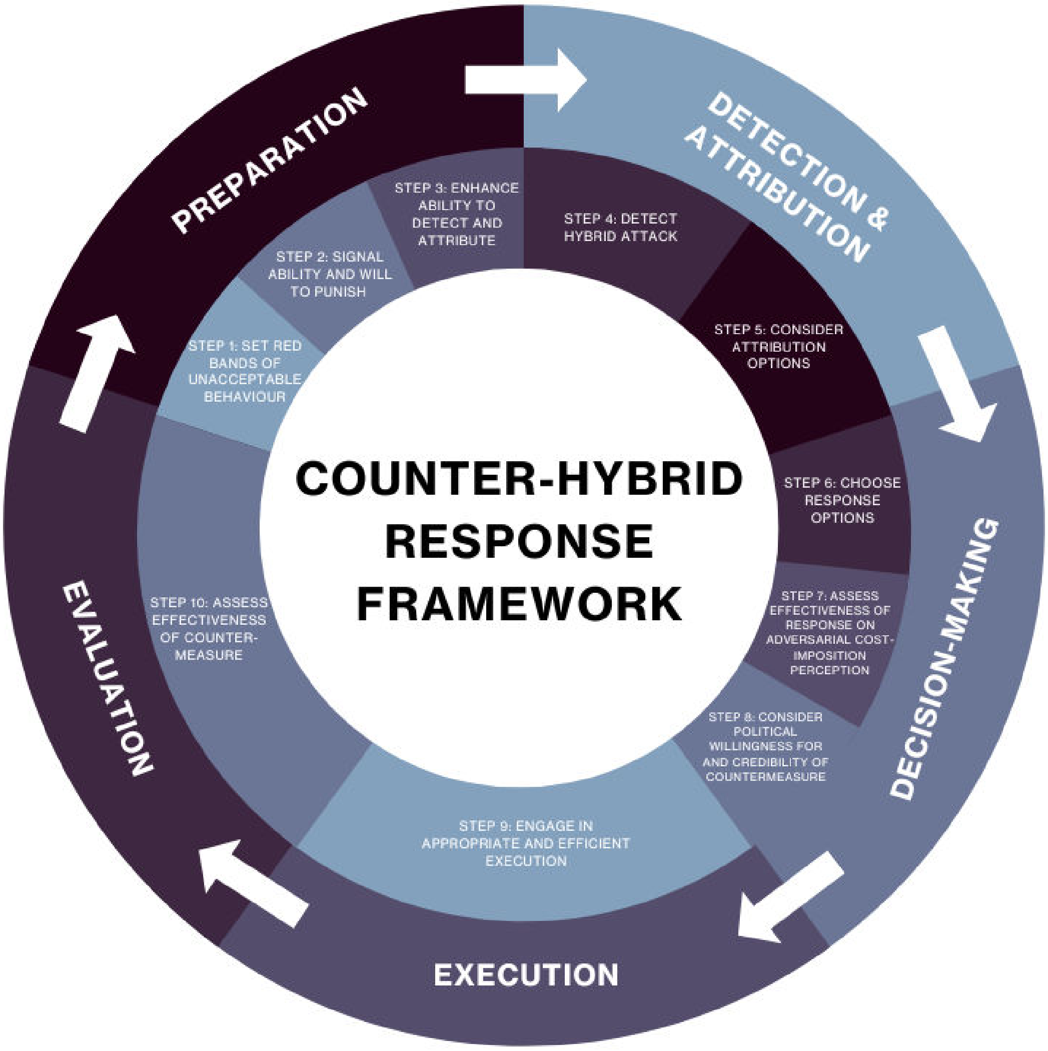
To address these pitfalls, this report provides a set of non-technical policy guidelines for a counter-hybrid posture for small and middle powers (SMPs) that explains how core good practices of cross-domain deterrence can be developed, applied and embedded into policies and practice. The report focuses specifically on active measures associated with deterrence by punishment to provide policymakers with useful insights to craft proportional and effective strategies to deal with actors operating in the grey zone. It also describes the steps needed to manage escalation and anticipate potential second- and third-order effects. Importantly, in conjunction with a counter-hybrid deterrence posture, positive reassurances and incentives should be communicated to the adversary to encourage good behaviour.

The Counter-Hybrid Response Framework

A five-stage response framework is proposed consisting of (i) the Preparation Stage, (ii) the Detection & Attribution Stage, (iii) the Decision-Making Stage, (iv) the Execution Stage, and (v) the Evaluation Stage. These stages are further subdivided into ten distinct steps, each including specific actions (see Table 1). The framework is circular in nature, capturing a continuous feedback loop to improve counter-hybrid measures going forward (see Figure 1). The focus is placed on deterrence by punishment, although links to other forms of deterrence (denial, entanglement, and norms) are considered. It is important to note that for SMPs especially, the execution of deterrence by punishment *campaigns* typically take place within multinational coalitions, which explains why the international context is explicitly taken into consideration. The framework provides practical guidelines to design effective counter-hybrid responses using different instruments of power across the DIMEFIL spectrum (i.e., Diplomatic, Information, Military, Economic, Financial, Intelligence, and Legal) while taking unintended second- and third-order effects into consideration.[1] It is worth noting that this model sets forth an ideal type of a counter-hybrid response framework. When putting a counter-hybrid posture into practice in the real world it is of paramount importance to remain flexible, improvise, and expect the unexpected when dealing with an ever-changing and dynamic opponent. Nonetheless, the proposed response framework offers practical guidelines to develop, apply, and embed good core practices of cross-domain deterrence into an effective counter-hybrid posture.

[1] See an extended introduction of and discussion on the DIMEFIL instruments of power in: Monika Gill, Ben Heap, and Pia Hansen, 'Strategic Communications Hybrid Threats Toolkit' (NATO Strategic Communications Centre of Excellence), 30–36, accessed 2 June 2022, https://stratcomcoe.org/publications/strategic-communications-hybrid-threats-toolkit/213.

Figure 1: The feedback loop of the five-stage, ten-step response framework.


PREPARATION
DETECTION & ATTRIBUTION
DECISION-MAKING
EXECUTION
EVALUATION
COUNTER-HYBRID RESPONSE FRAMEWORK
STEP 1: SET RED BANDS OF UNACCEPTABLE BEHAVIOUR
STEP 2: SIGNAL ABILITY AND WILL TO PUNISH
STEP 3: ENHANCE ABILITY TO DETECT AND ATTRIBUTE
STEP 4: DETECT HYBRID ATTACK
STEP 5: CONSIDER ATTRIBUTION OPTIONS
STEP 6: CHOOSE RESPONSE OPTIONS
STEP 7: ASSESS EFFECTIVENESS OF RESPONSE ON ADVERSARIAL COST-IMPOSITION PERCEPTION
STEP 8: CONSIDER POLITICAL WILLINGNESS FOR AND CREDIBILITY OF COUNTERMEASURE
STEP 9: ENGAGE IN APPROPRIATE AND EFFICIENT EXECUTION
STEP 10: ASSESS EFFECTIVENESS OF COUNTER-MEASURE

(i) The Preparation Stage

The Preparation Stage involves articulating core interests and communicating red bands of unacceptable behaviour to an opponent. It furthermore requires building up and enhancing the capability to detect hybrid attacks and the political will to attribute them.

Step 1: Set red bands of unacceptable behaviour, which maintain a degree of strategic ambiguity. This clearly communicates to an opponent what behaviour could trigger a response, whilst at the same time preventing the opponent from abusing tightly defined redlines and engaging in salami tactics. Thereby, defenders educate their adversaries, whilst preventing abuse. Moreover, provide positive reassurances and incentives to encourage good behaviour, and engage in norm-setting.

Step 2: Communicate publicly or privately one's capability and will to retaliate against hybrid threats should a threshold be crossed.

Step 3: Boost the capability to detect hybrid aggression, as well as enhance willingness to meaningfully attribute such conducts at the political level.

(ii) The Detection & Attribution Stage

The Detection and Attribution Stage focuses on the detection of hybrid attacks and the subsequent attribution of the attack to an opponent.

Step 4: Detect the hybrid attack by implementing the detection capabilities developed in the Preparation Stage based on effective intelligence sharing with partners.

Step 5: Consider the attribution options and decide whether and to what extent attribution is desirable. If one chooses to attribute, do so effectively within a politically meaningful timeframe, and explain it convincingly to third parties to garner support.

(iii) The Decision-Making Stage

The Decision-Making Stage is pivotal in any successful counter-hybrid strategy and is divided into three different steps.

Step 6: Choose response options across the entire spectrum and identify possible targets. Each response option includes consideration of (i) the legality of the action, (ii) the duration and timeframe within which it comes into effect, (iii) the proportionality of the countermeasure, (iv) entanglements and second- and third-order effects, and (v) an escalation assessment.

Step 7: Assess the effectiveness of the response on adversarial cost-imposition perception. Policymakers must evaluate and assess whether the measures are likely to affect the cost-benefit calculus of the specific aggressor one seeks to deter.

Step 8: Ensure that there is enough political support and willingness for the countermeasure and confirm that the aggressor(s) perceive(s) the retaliatory threats as credible.

(iv) The Execution Stage

In the Execution Stage, the response option is executed and countermeasures are implemented.

Step 9: Execute the chosen response option. Responses should be implemented in a timely manner to warn aggressors with reference to the interests that the responder seeks to protect and further threats it is willing to execute. Domestic and international support for the chosen response should be monitored and strategic goals should be kept at the centre. The implementation is complemented by synchronised government-wide, multilevel strategic communication (StratCom), unless covert action is chosen.

(v) The Evaluation Stage

In the Evaluation Stage, the entire process is evaluated.

Step 10: Assess the effectiveness of the countermeasure. The step includes evaluating the obtainment of the cost-imposition objectives, assessing escalatory dynamics, and considering second- and third-order effects. (see Table 1)

The Way Forward

Over the past decade, policy efforts to counter hybrid threats within Western SMPs have had considerable momentum. Counter-hybrid units were created, budgets allocated, strategies drafted, national and international consultation and coordination mechanisms established, a growing body of legal frameworks adopted, and an assortment of policy measures implemented. All these efforts contributed to the goal of addressing hybrid threats designed to circumvent detection, existing rules and regulation, and response thresholds in order to minimise the basis for decisive responses. The counter-hybrid toolbox of Western SMPs now include preventive resilience as well as proactive response measures including the punishment of violations with the intention to deter their future occurrence.

The policy guidelines offered in this report will help inform the execution of the deterrence component of SMP's counter-hybrid postures. The guidelines offer practical insights on how to craft and execute proportional, legitimate, and effective countermeasures to deter actors operating in the grey zone, while simultaneously managing escalation and anticipating potential second- and third-order effects. The design and execution of such countermeasures need to be synchronised between different branches of government, require close cooperation with international partners, and will sometimes necessitate the involvement of private sector actors. Now is the time to take the next step in the counter-hybrid policy realm. To that purpose, we offer three recommendations to policymakers in SMPs to take this forward:

1. Convene an international symposium with representatives from SMPs to discuss how these policy guidelines can guide the further development of counter-hybrid efforts at the national and the international level. The Counter Hybrid Threat Centre of Excellence in Helsinki is well positioned to spearhead this effort.

2. Adopt and adapt these policy guidelines to the context of specific institutional and policy planning cycles. This, of course, lies within the national competencies of individual SMPs.

3. Deploy the policy guidelines within the context of a real-world counter-hybrid campaign. Such a campaign can be executed by individual SMPs or, as suggested in this report, by SMPs closely working together with partners in bilateral and multilateral partnerships. It is recommended that The Netherlands in collaboration with one or multiple selected partner countries takes the lead in this endeavour. Such campaigns can first be practiced in simulations and serious gaming.

Now is the time to take the next step in the counter-hybrid policy realm.

Table 1: The actions required in each step of the response framework. An extended discussion of each step can be found in the full report below.

Stages	Steps	Actions
Preparation	**Step 1: Set red bands of unacceptable behaviour**	1. Parse the spectrum of adversarial hybrid operations based on their impact, marking which ones will prompt a response. 2. Set red bands of unacceptable behaviour 3. Communicate the red bands of unacceptable behaviour internally, with partners, and possibly with adversaries. 4. Encourage positive behaviour through reassurances, incentives, and norm setting.
	Step 2: Signal ability and will to punish	5. Signal ability and will to deliver on deterrence promises, possibly through the demonstration of capability and announcement of commitment.
	Step 3: Enhance ability to detect and attribute	6. Increase detection capability. 7. Strengthen ability to attribute within a politically meaningful timeframe. 8. Prepare to convincingly explain attribution to third parties.
Detection & Attribution	**Step 4: Detect hybrid attack**	9. Detect hybrid attack.
	Step 5: Consider attribution options	10. Decide whether to attribute. 11. Attribute in an effective manner.
Decision-making	**Step 6: Choose response options**	12. Parse the available countermeasures across the DIMEFIL spectrum according to their impact. 13. Identify possible targets across multiple domains, including counterforce, countervalue, and counter-political targets. 14. Assess the legality of the response options. 15. Assess the duration and the timeframe within which they come into effect. 16. Consider the proportionality of the countermeasure. 17. Identify entanglements and second- and third-order effects. 18. Conduct an escalation assessment.
	Step 7: Assess effectiveness of response on adversarial cost-imposition perception	19. Examine costs at the psychological level. 20. Examine costs at the political level. 21. Examine costs at the economic and operational level.
	Step 8: Consider political willingness for and credibility of countermeasure	22. Assess the credibility of the countermeasure in the eyes of the opponent. 23. Assess the political willingness to adopt the countermeasure. 24. Synchronise and coordinate domestic efforts: *whole-of-government* and *whole-of-society.* 25. Synchronise and coordinate international efforts.
Execution	**Step 9: Execute response option and implement countermeasures**	26. Implement a timely warning response with reference to vital interests and threat of punishment. 27. Monitor domestic and international support. 28. Keep strategic goals at the centre. 29. Execute synchronised and coordinated government-wide, multilevel StratCom.
Evaluation	**Step 10: Assess effectiveness of countermeasure**	30. Evaluate attainment of cost-imposition objective. 31. Evaluate escalatory dynamics. 32. Evaluate second- and third-order effects.

1. Introduction

Rival states increasingly use hybrid tactics to exploit vulnerabilities and influence democratic processes. These tactics include the coordinated and synchronised use of violent and non-violent instruments of power to execute cross-domain activities, often circumventing detection and attribution, that are conducted below the threshold of conventional armed military conflict. Fast-paced technological development and deep globalisation have provided rival states with startling tools to erode the democratic processes and institutions of foreign competitors.

Rival states increasingly use hybrid tactics to exploit vulnerabilities and influence democratic processes.

In recent years, Western states have increased their situational awareness and noted the need to guard against potential hybrid threats. For example, the North Atlantic Treaty Organisation's (NATO) latest Strategic Concept launched at the Summit of Madrid in June 2022 reaffirms the Alliance members' determination to counter hybrid threats, highlighting plans to 'invest in our ability to prepare for, deter, and defend against the coercive use of political, economic, energy, information and other hybrid tactics by states and non-state actors'.[2] Governments acknowledge that bolstering defences and enhancing resilience does not suffice to deter hybrid aggressors. As a result, their counter-hybrid policies have evolved and have started to encompass more proactive policies, including those specifically aimed at deterrence.

However, deterring hybrid aggressors is a difficult task. Not least because hybrid adversaries deliberately circumvent detection and escape responsibility, there are no clear shared rules that regulate acceptable behaviour, defenders lack either the capability or the willingness to respond, defenders lack a proper understanding of both the incentive structure and weak spots of rival actors, and the design and execution of counter-hybrid policies often come with potential second- and third-order effects. Therefore, it is of paramount importance to develop a proactive counter-hybrid deterrence posture, which addresses these pitfalls. This will improve states' ability to guard against potential hybrid threats going forward.

[2] NATO, 'NATO 2022 - Strategic Concept' (NATO, June 2022), 7.

1.1 Disentangling core concepts: definitions and meanings

Before turning to the framework, it is important to expound on the key concepts central to this report, including 'hybrid' threats and 'deterrence'. 'Hybrid' or 'grey zone'[3] operations feature 'the simultaneous employment of military and non-military instruments, typically below the conventional military threshold, to exploit adversary's vulnerabilities, in the pursuit of political objectives'.[4] Operations below the threshold of conflict are usually conducted in domains that 'cover the full spectrum of modern domestic and international life' to exploit cross-domain interconnectedness and entanglement. Consequently, hybrid threats are increasingly 'difficult to distinguish from one-off actions, statecraft, or diplomacy',[5] thus significantly hampering a defender's ability to detect and attribute offensive behaviours.

Deterrence, on the other hand, is broadly defined as 'the practice of discouraging or restraining someone from taking unwanted actions'[6] and it is usually achieved by 'persuading an adversary that prospective costs would outweigh prospective gains'.[7] Although related, deterrence differs from *compellence*. Both rely on the use of threats to shape the aggressor's behaviour. However, while deterrence 'demands that the adversary refrains from acting',[8] compellence implies 'an effort to force an actor to *do* something'.[9] Traditional scholarship within conventional and nuclear contexts differentiates between *deterrence by punishment* and *deterrence by denial*. Deterrence by punishment implies the threat of 'severe penalties, such as nuclear escalation or severe economic sanctions, if an attack occurs',[10] and it aims 'to influence future events, to demonstrate that objectionable acts have consequences'.[11] Deterrence by denial, in turn, involves 'strategies to deter an action by making it infeasible or unlikely to succeed, thus denying a potential aggressor confidence in attaining its objectives'.[12]

It is widely accepted that effective deterrence is not a simple rational decision-making process. The traditional game-theoretic models of deterrence based on a 'mathematical'

[3] The terms 'hybrid conflict' and 'grey zone' are often used interchangeably, but have different meanings and origins. For more on this, see: Frank Hoffman, 'Examining Complex Forms of Conflict: Gray Zone and Hybrid Challenges', *PRISM* 7, no. 4 (8 November 2018): 31–47. This report uses the definition of 'hybrid' offered by the European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE), see: Centre of Excellence, 'What Is Hybrid CoE?', *Hybrid CoE - The European Centre of Excellence for Countering Hybrid Threats* (blog), accessed 13 December 2022.; see also NATO, 'Capstone Concept for the Military Contribution to Countering Hybrid Threats' (NATO, 25 August 2010). The Netherlands defines hybrid conflicts as 'conflicts between states, largely below the legal level of armed conflict, with integrated use of civilian and military means and actors, with the aim of achieving certain strategic objectives.' Translation of the Dutch definition taken from Nationaal Coördinator Terrorismebestrijding en Veiligheid, 'Chimaera: een duiding van het fenomeen "hybride dreiging"', (Ministerie van Justitie en Veiligheid, 18 April 2019).

[4] Sweijs and Zilincik, 'The Essence of Cross-Domain Deterrence', 131.

[5] Lindsey R. Sheppard and Matthew Conklin, 'Warning for the Gray Zone' (Centre for Strategic & International Studies, 2019).

[6] Michael J. Mazarr, 'Understanding 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, NL ARMS (The Hague: T.M.C. Asser Press, 2021), 15.

[7] Lawrence Freedman, 'Introduction — The Evolution of Deterrence Strategy and Research', in *NL ARMS Netherlands Annual Review of Military Studies 2020*, ed. Frans Osinga and Tim Sweijs, NL ARMS (The Hague: T.M.C. Asser Press, 2021), 5.

[8] Gary Schaub, 'Deterrence, Compellence, and Prospect Theory', *Political Psychology* 25, no. 3 (2004): 389.

[9] Mazarr, 'Understanding Deterrence,' 15.

[10] Mazarr, 'Understanding Deterrence,' 15.

[11] Becca Wasser et al., eds., *Comprehensive Deterrence Forum: Proceedings and Commisioned Papers*, Conference Proceedings, CF-345-A (Santa Monica, Calif: RAND Corporation, 2018), 25.

[12] Mazarr, 'Understanding Deterrence,', 15.

cost-benefit calculus fall short of grasping the underlying psychological and cognitive elements that determine how behaviours are executed.[13] Indeed, any deterrence strategy must be grounded in a thorough understanding of the role that respective perceptions and psychological motivations play in that particular context. The objective of deterrence is, indeed, to make an adversary *perceive* '[...] that the costs likely to be incurred from his initiative will outweigh the potential gains'.[14] Therefore, the material capability to accomplish retaliatory threats and deny an aggressor meaningful gains is somewhat subordinate to the ability to convinve an adversary at the psychological level that it has no other choice than to refrain from taking a certain action. This highlights the importance of strategic communication.[15] An adversary's resolve to attack is shaped by several factors, including the fear of undermining its position, either in the international or the domestic arena, as well as potential ideological inclinations of a leader that colour his perception.[16] Consequently, successful deterrence strategies must be tailored to the interests, preferences, and risk propensity of the specific actor, either state or non-state, that one seeks to deter.[17] Policymakers should then provide answers not only to 'what might the adversary do?', but, more importantly, to 'how might the adversary interpret my actions and why?'.[18]

Effectively deterring hybrid aggressors remains difficult.

To integrate the deterrence rationale into the hybrid domain, theoretical and conceptual innovations to the traditional understanding of deterrence have been added. First, there is an increased awareness and consequent need to accept that relevant hybrid activities – such as disinformation and cyber operations – may not be deterred in absolute terms. In this sense, unavoidable threats and their cross-domain essence propelled a refinement and expansion of traditional resilience strategies to encompass concepts such as those of *tactical* and *strategic denial*.[19] In this regard, denial is no longer understood as a purely defensive setting but rather as a strategy to impose costs by 'denying [the hostile] the political benefits that it expects to derive' from aggressive behaviours. Second, the traditional understanding of punishment, developed in the conventional-nuclear domain has been significantly expanded to meet new cross-domain challenges emerging in the grey zone. Deterrence strategies based on punishment now encompass *deterrence through norms*, *delegitimisation*, and *entanglement*. Deterrence through norms aims to '[...] alter the cost calculus of those who do not abide by the positive standards of behaviour [...]'[20]. Delegitimisation is a form of punishment that involves the use of naming and shaming or stigmatisation to raise the aggressor's cost-benefit calculus 'by challenging the normative, religious, and socio-political rationales individuals rely upon [...]'.[21] Finally, deterrence through entanglement leverages cross-domain interdependencies between states due to globalisation and international cooperation. As Joseph Nye puts it, 'interdependences make a successful attack simultaneously impose serious costs on the

[13] Jeffrey D. Berejikian, 'A Cognitive Theory of Deterrence.' Journal of Peace Research 39, no. 2 (2002): 165-83.

[14] Dorthe Bach Nyemann and Heine Sorensen, 'Going Beyond Resilience. A Revitalised Approach to Countering Hybrid Threats', Hybrid CoE Strategic Analysis (Hybrid CoE, 8 January 2019).

[15] Robert Jervis, 'Deterrence and Perception', *International Security* 7, no. 3 (1982): 4.

[16] Richard Ned Lebow, 'The Deterrence Deadlock: Is There a Way Out?', *Political Psychology* 4, no. 2 (1983): 333–54.

[17] Michael J. Mazarr et al., 'What Deters and Why: Exploring Requirements for Effective Deterrence of Interstate Aggression' (RAND Corporation, 20 November 2018).

[18] UK Ministry of Defence, 'Joint Doctrine Note 1/19, Deterrence: The Defence Contribution', GOV.UK, 2019, 8.

[19] Matthew Kroenig and Barry Pavel, 'How to Deter Terrorism', *The Washington Quarterly* 35, no. 2 (April 2012): 31. In the context of deterrence against terrorism, the Authors consider tactical denial to threaten failure at the tactical level. In contrast, strategic denial is understood as threatening to deny the opponent the strategic benefits it aims to achieve, even in the face of a successful attack.

[20] Sweijs and Zilincik, 'The essence of Cross-Domain Deterrence', 149.

[21] Alex S. Wilner, 'Deterring the Undeterrable: Coercion, Denial, and Delegitimization in Counterterrorism', *Journal of Strategic Studies* 34, no. 1 (1 February 2011): 27.

attacker as well as the victim.'[22] The core assumption is, therefore, that actors entangled in dependencies will likely refrain from launching attacks because they will inevitably incur costs, be it real or perceived.

However, effectively deterring hybrid aggressors remains difficult. There are different reasons for this. First, hybrid adversaries deliberately circumvent detection and escape responsibility. Second, no clear shared rules exist that regulate acceptable behaviour, which hybrid aggressors subsequently exploit. Third, defenders lack either the capability or will to respond. Fourth, defenders lack a proper understanding of both the incentive structure and weak spots of rival actors and are consequently unable to design tailored and effective policies that hit the opponent where it hurts. Furthermore, defenders are not able to convincingly communicate counter-hybrid policies beforehand. Fifth, the design and execution of counter-hybrid policies often come with potential second- and third-order effects that are not always immediately clear, and a robust understanding of their escalatory dynamics is lacking. This further complicates the design and execution of counter-hybrid policies.

To address these pitfalls, this document provides a non-technical, ten-step, 'how to' policy guidelines of a counter-hybrid posture that explains how core good practices of deterrence can be developed, applied and embedded into policies and practice. The report focuses on active measures that fall under *deterrence by punishment* to provide policymakers with useful insights to craft proportional and effective strategies to deter actors operating in the grey zone while simultaneously managing escalation and anticipating potential second- and third-order effects. In addition, these guidelines treat counter-hybrid deterrence as an iterated game, in which defender and challenger continuously interact through attacks and counterattacks. Even though red bands of unacceptable behaviour are set, we assume that adversaries may cross them. Therefore, the goal of creating a counter-hybrid posture is to achieve cumulative deterrence, where one shapes the strategic behaviour of an opponent over the long term and sets the basis for an improved strategic situation.[23] In short, these guidelines offer policymakers and practitioners a framework of best practices for designing, selecting, and implementing countermeasures to counter-hybrid threats.[24]

In the following chapter, the five stages of the counter-hybrid response framework will be discussed in detail, namely the (i) Preparation, (ii) Detection & Attribution, (iii) Decision-Making, (iv) Execution, and (v) Evaluation Stage. Each of the ten steps will be expanded on by considering the different actions that need to be taken. The last chapter offers concluding thoughts on the way forward. In doing so, this report sets forth key practical insights to improve counter-hybrid postures and guard against hybrid threats.

[22] Joseph S. Nye, 'Can China Be Deterred in Cyber Space?', *EastWest Institute* (blog), 2 February 2016.

[23] Doron Almog, 'Cumulative Deterrence and the War on Terrorism', *The US Army War College Quarterly: Parameters* 34, no. 4 (1 November 2004), https://doi.org/10.55540/0031-1723.2222.

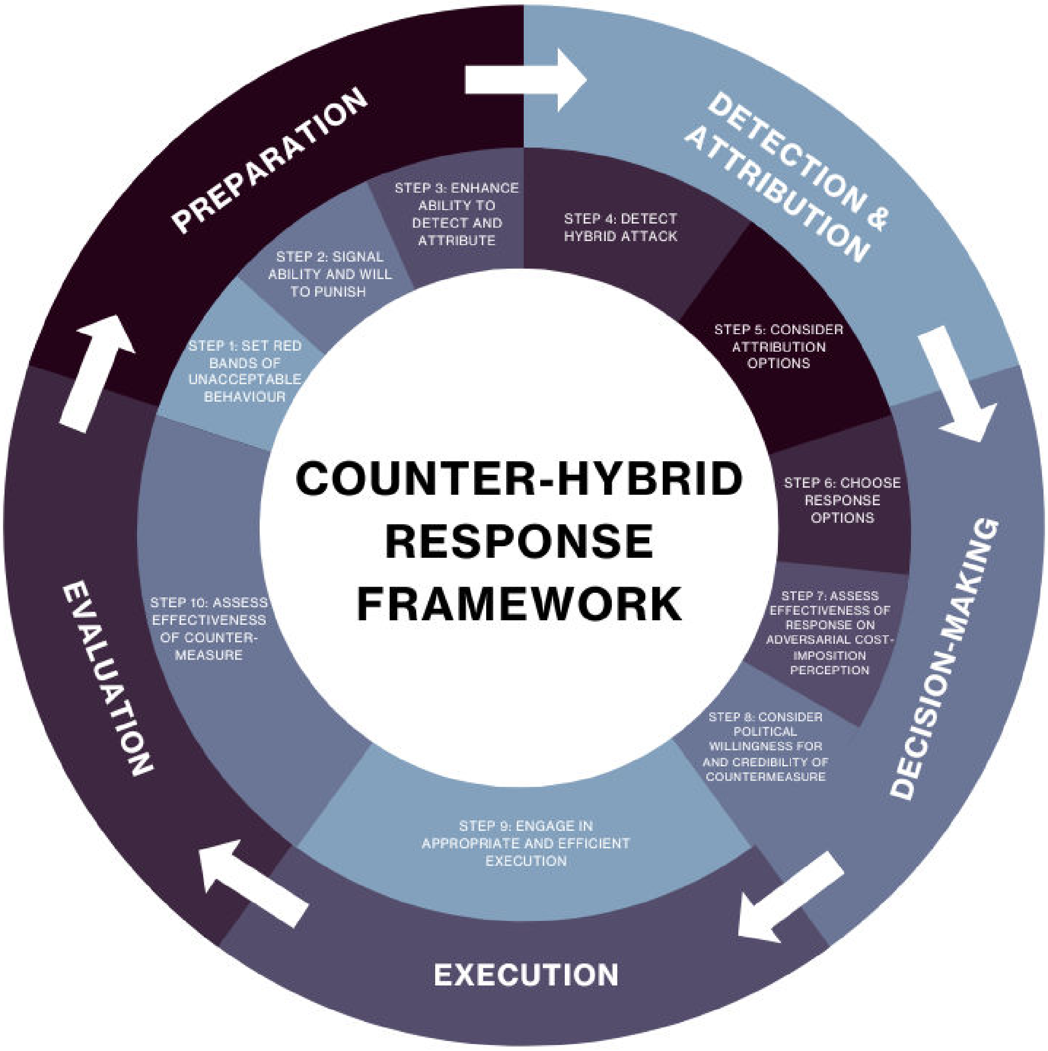
[24] Countermeasures in this policy guideline refer to the full range of countermeasures that defenders can employ across the entire DIMEFIL spectrum.

2. The Counter-hybrid Response Framework

This chapter proposes a five-stage framework to provide insights that can help guide policymakers in the (i) Preparation, (ii) Detection & Attribution, (iii) Decision-Making, (iv) Execution, and (v) Evaluation Stages of counter-hybrid responses, which are conveniently subdivided into ten detailed steps (see Figure 2). The focus is placed on deterrence by punishment while taking into consideration the link to other forms of deterrence (denial, entanglement, and norms). It is important to note that this framework treats counter-hybrid deterrence as an iterated game, in which defender and challenger continuously interact through attacks and counterattacks. Even though red bands of unacceptable behaviour are set, we assume that adversaries may cross them. Therefore, the goal of creating a counter-hybrid posture is to achieve cumulative deterrence, where one shapes the strategic behaviour of an opponent over the long term and sets the basis for an improved strategic situation.[25] Moreover, for SMPs especially, the execution of deterrence by punishment campaigns typically take place within multinational coalitions. The proposed framework provides practical guidelines to design effective counter-hybrid responses across the DIMEFIL spectrum (Diplomatic, Information, Military, Economic, Financial, Intelligence, and Legal) while taking unintended second- and third-order effects into consideration. Each step includes specific actions, which are discussed in more detail in sections 4 through 8.

[25] Almog, 'Cumulative Deterrence and the War on Terrorism'.

Figure 2: The feedback loop of the five-stage, ten-step response framework.


PREPARATION
DETECTION & ATTRIBUTION
DECISION-MAKING
EXECUTION
EVALUATION
STEP 1: SET RED BANDS OF UNACCEPTABLE BEHAVIOUR
STEP 2: SIGNAL ABILITY AND WILL TO PUNISH
STEP 3: ENHANCE ABILITY TO DETECT AND ATTRIBUTE
STEP 4: DETECT HYBRID ATTACK
STEP 5: CONSIDER ATTRIBUTION OPTIONS
STEP 6: CHOOSE RESPONSE OPTIONS
STEP 7: ASSESS EFFECTIVENESS OF RESPONSE ON ADVERSARIAL COST-IMPOSITION PERCEPTION
STEP 8: CONSIDER POLITICAL WILLINGNESS FOR AND CREDIBILITY OF COUNTERMEASURE
STEP 9: ENGAGE IN APPROPRIATE AND EFFICIENT EXECUTION
STEP 10: ASSESS EFFECTIVENESS OF COUNTER-MEASURE
COUNTER-HYBRID RESPONSE FRAMEWORK

2.1 The Preparation Stage

The Preparation Stage involves articulating core interests and communicating red bands of unacceptable behaviour to an opponent. It furthermore requires building up and enhancing the capability to detect hybrid attacks and the political will to attribute them.

Set red bands of unacceptable behaviour, whilst maintaining a degree of strategic ambiguity

2.1.1 Step 1: Set red bands of unacceptable behaviour

The first step in the Preparation Stage is to set red bands of unacceptable behaviour, whilst maintaining a degree of strategic ambiguity. This must not only be signalled by use of Cold War-style public statements but through a combination of overt and covert, explicit and implicit means at both domestic and international policy levels. Small and medium-sized powers, such as the Netherlands, should seek like-minded partners and operate within broader international frameworks, such as the European Union, to set these red bands of unacceptable behaviour in concert with other states.

Parse the spectrum of adversarial hybrid operations based on their impact, marking which ones will prompt a response

A defender must assess which specific hybrid operations would affect its vital interests and, consequently, require an immediate response. When determining the spectrum of possible hybrid operations, the defender must evaluate which ones can truthfully be executed and which ones cannot. Following such evaluation, the defender must collect all possible hybrid operations and mark the ones that would prompt a response based on their impact on vital national interests or the interests of their partners. In addition, smaller states should seek out the red bands of unacceptable behaviour of like-minded partners and note synergies, identifying the red bands that could be set in concert with other states.

Set red bands of unacceptable behaviour

Once the menu of potential threats has been identified and linked to national interests, defenders must make clear what is unacceptable behaviour, using red bands of unacceptable behaviour in order to prevent opponents from abusing redlines and engaging in salami tactics. Thereby, defenders educate their opponents, whilst preventing abuse, and simultaneously rally support among a coalition of the willing to retaliate in case of aggression. Smaller states, such as the Netherlands, should seek to set these red bands in conjunction with other like-minded partners. A clear example can be drawn from the recent joint efforts in countering cyber threats at the EU level, which translated into the EU Cyber Diplomacy Toolbox.[26]

It is important to maintain a reasonably narrow degree of ambiguity as this is preferable at the communicative level to prevent abuse by opponents.

It is important to maintain a reasonably narrow degree of ambiguity as this is preferable at the communicative level to prevent abuse by opponents. Setting clear redlines might incentivise adversaries to exploit cross-domain interconnectedness and design operations that steer clear from those set thresholds, thus frustrating a defender's efforts to deter a specific aggressive behaviour in the first place. Second, strict redlines may be imprecise and unverifiable due to the hybrid domain's highly volatile and ambiguous characteristics and the operations carried out therein.[27] For instance, Article 5 of the North Atlantic Treaty, which provides that an 'armed attack' would trigger a collective response by NATO member states, proves an effective deterrent in the conventional domain. However, translating Article 5 into the hybrid context is more difficult. Although the Alliance has publicly stated that 'hybrid actions against one or more Allies could lead to a decision to invoke Article 5 of the North Atlantic Treaty'[28], it is difficult to ascertain the exact actions that would trigger Article 5.

Therefore, instead of strict redlines, states could set red bands of unacceptable behaviour to signal what they are trying to deter and how they aim to protect their vital interests. This can be achieved by establishing a clear normative framework detailing what constitutes accepted behaviour – either through domestic policy and norms, or through international cooperation, agreements, and diplomacy. Compared to the identification of strict redlines, red bands provide the defender with greater room for manoeuvre when responding. Furthermore, a lower degree of specificity and the choice not to commit to a specific response action also limits the possibilities for the adversary to circumvent such objectives, instrumentalise narratives, and trigger escalation. Yet, while loose communication may prove successful and easy to achieve at the domestic level, it also bears inherent limits when projected onto the

[26] 'The EU Cyber Diplomacy Toolbox', accessed 16 November 2022.

[27] Daniel W. Altman, 'Redlines and Faits Accomplis in Interstate Coercion and Crisis' (Thesis, Massachusetts Institute of Technology, 2015).

[28] NATO, 'NATO's Response to Hybrid Threats', NATO, 21 June 2022, https://www.nato.int/cps/en/natohq/topics_156338.htm.

international stage. Indeed, current developments in cyber warfare and cyber deterrence demonstrate that, whenever powerful competitors sit at the table to discuss the establishment of rules of conduct and good behaviour, reaching consensus – or even a broadly shared agreement – can be extremely difficult.[29]

Communicate the red bands of unacceptable behaviour internally, with partners, and possibly with adversaries

Once the red bands of unacceptable behaviour are set, they must be backed with credible threat of enforcement and should be properly communicated – both internally and externally – to signal the will and commitment to engage with foreign aggressive behaviours. Communicative efforts should be undertaken beforehand, in peacetime, as a constant reminder of a defender's commitment to retaliate in conjunction with meaningful strategic communication and public diplomacy. Communication may take place either overtly or covertly and through public or private means. The decision about which means and ways to communicate should be the result of a thorough assessment of the relevant circumstances. This approach avoids translating deterrence threats into a 'general policy of hostility' that the adversary could instrumentalise and weaponise.[30]

Red bands of unacceptable behaviour are set, they must be backed with credible threat of enforcement.

It is important to communicate red bands of unacceptable behaviour internally and externally, to both likeminded partners and – most importantly – the adversary. With regards to the former, communicative efforts must aim to involve the broader society and population to enhance threat awareness and signal the state's 'preparedness to respond'.[31] Then, thresholds should be disseminated across partners and allies to gain support at the international level and isolate hostile competitors. Finally, adversaries should also be aware of which conducts are likely to trigger retaliatory responses.

Encourage positive behaviour through reassurances, incentives, and norm setting

In conjunction with red bands of unacceptable behaviour, positive reassurances and incentives should also be communicated to the adversary, as well as setting norms. If an adversarial state withholds from crossing stated red bands and complies to behavioural benchmarks, positive reassurances and incentives, as well as the setting of norms, should encourage an opponent to engage in positive behaviour. Such reassurances and incentives can be provided in various domains, including the use of economic, political, and legal incentives.[32] By using this in combination with red bands of unacceptable behaviour, strategies of deterrence and compellence are used in tandem. Whilst the red bands demand that the adversary refrains from acting, the positive incentives and norm setting compel an adversary to adhere to these red bands through positive behaviour.

[29] Ann Väljataga, 'Back to Square One? The Fifth UN GGE Fails to Submit a Conclusive Report at the UN General Assembly', *NATO Cooperative Cyber Defence Centre of Excellence* (blog), accessed 13 June 2022.

[30] Mazarr, 'Understanding Deterrence', 9.

[31] Vytautas Keršanskas, 'Deterrence: Proposing a More Strategic Approach to Countering Hybrid Threats', Hybrid CoE Paper 2 (March 2020), 24.

[32] James Pattison, 'Positive Incentives', in *The Alternatives to War: From Sanctions to Nonviolence*, vol. 1 (Oxford University Press, 2018).

2.1.2 Step 2: Signal ability and will to punish

Signal ability and will to deliver on deterrence promises, possibly through the demonstration of capability and announcement of commitment

In the second step, defenders must signal their ability and willingness to punish. At political and strategic levels, signalling takes the form of public and private declarations, the publication of national strategies or doctrines in which reactions are linked to actions, as well as norm development. Defenders must ensure that, whatever the specific measure adopted, they effectively signal both their capability and political resolve to retaliate, without being perceived as a disproportionate threat or provocation.[33] This not only demonstrates a serious commitment to retaliate but it also prevents presenting aggressors with a *fait accompli*. For instance, in a recent letter to the parliament, the Dutch Minister of Foreign Affairs clearly stated that, under strict legal conditions, the Defence Cyber Command is allowed to use offensive cyber capabilities against aggressive state actors.[34] The statement followed innovative developments embedded in the Dutch 2018 Cyber Strategy, which highlighted the role of offensive capabilities for deterrence purposes.[35] While the publication of formal defence strategies and doctrines is a powerful way to overtly communicate one's posture, states routinely perform actions – such as the conclusion of international agreements, the establishment of diplomatic and economic relations with third parties, etc. – without the intention of expressly communicating something. The basic assumption, then, is that everything communicates in the hybrid context and recent technological developments have favoured the dramatic increase in available communication channels. As a general rule of thumb, communications must be clear and specific.[36] If messages are clear and specific, it is likely that the aggressor will effectively perceive what the defender is trying to accomplish. This significantly reduces the risk of misunderstanding and ambiguity, thus avoiding unintended provocation and escalation.[37]

In the conventional realm, effective signalling is much easier to accomplish than in the hybrid context.

In the conventional realm, effective signalling is much easier to accomplish than in the hybrid context. In addition to political declarations, signalling in the conventional realm occurs through the deployment of military forces in or nearby disputed territories, the acquisitions of weapons, or by building and declaring the possession of innovative capabilities, such as planes, drones or other kinetic devices. The situation is radically different in the hybrid context. Firstly, given the nature of hybrid threats, the use of the military to signal a resolve to retaliate appears to be disproportionate and is inevitably prone to quick escalation. Secondly, and more significantly, signalling in such a blurred and cross-entangled environment can be extremely challenging simply because it is harder to design warnings about particular actions

[33] In the conventional domain, the invasion of Kuwait by Iraqi forces in 1990 and, in general, the events that occurred between 1990 and 2003, are commonly viewed as an egregious failure by the U.S. to clearly set warnings that could have deterred Saddam Hussein. The failure must be traced to the confusing and contradictory terms in which the U.S. framed its relationship with Iraq, as well as to a clear misunderstanding and underestimation of the opponent's strategic interests in annexing the territory of Kuwait. See Daniel R. DePetris, 'When Deterrence Failed: Why Saddam Hussein Invaded Kuwait', Text, *The National Interest* (blog) (The Center for the National Interest, 27 November 2018).

[34] H.P.M. Knapen, 'Tegenmaatregelen ransomware-aanvallen', Tweede Kamer der Staten Generaal, October 2021.

[35] Ministerie van Defensie, 'Defensie Cyber Strategie 2018 - Investeren in digitale slagkracht Nederland' (Ministerie van Defensie, 12 November 2018).

[36] Aaron Brantly, 'Back to Reality: Cross Domain Deterrence and Cyberspace', SSRN Scholarly Paper (Rochester, NY, 1 September 2018), 5.

[37] Chinese military intervention in Korea in 1950 is a clear example of unclear communication which inevitably escalated the ongoing conflict. In that occasion, the U.S./United Nations failed to clearly communicate what they were seeking to deter and, despite evident unbalances in military forces and the threat of a potential nuclear retaliation, Chinese strongly motivated leaders accepted such risk and resolved to intervene. See, in this regard, Michael E. Brown, 'Deterrence Failures and Deterrence Strategies: Or, Did You Ever Have One of Those Days When No Deterrent Seemed Adequate?' (RAND Corporation, 1977), 13.

that the defender wants to deter in one domain with retaliatory threats envisaged in a different domain. Therefore, there is a serious risk of generating misunderstanding.[38] For instance, the very backbone of the Internet – in which neither the deterrer nor the aggressor exert direct control over the relevant infrastructure – makes signalling in cyberspace difficult, because cyber signals are likely to get lost or ignored by the targeted audience.[39] On the same token, overtly signalling one's cyber attribution capabilities or offensive arsenals is likely to prove detrimental, since it inevitably prompts adversaries to craft alternative solutions to circumvent defences.[40] Drawing lessons from the reciprocal pre-positioning that the U.S. and Russia have been carrying out in the past years within each other's critical infrastructures, it appears that an effective way to send warnings in cyberspace is to disclose the possession of offensive capabilities or the threat of retaliation once the action has already occurred.[41]

On a different note, signalling against economic coercion usually requires a significant amount of time, especially when efforts are undertaken at the regional or international levels. In this regard, it is worth mentioning that the EU – after a consistent release of public statements and declarations in the past years – is currently developing norms to clearly signal that it is not willing to tolerate economic coercion any longer. The Commission's proposal on the establishment of a dedicated regulation against economic coercion[42] is a clear signal that the EU is willing to shift from a purely denial posture – which traditionally occurred through the establishment of a foreign direct investments screening tool[43] – to a proactive deterrence by punishment one.

A straightforward yet partial solution to some of the challenges mentioned is that signalling in the hybrid context should be cross-domain and occur continuously. Effective signalling in the hybrid context requires a 'synergistic employment of communication across more levels than previously'.[44] In this sense, defenders must take advantage of an integrated whole-of-government posture to constantly synchronise warnings and communicative efforts to boost clarity and credibility. Significant insights in this regard, can be drawn from the orchestrated effort that the U.S. deployed across different levels to warn China that it was not willing to accept economic espionage and intellectual property (IP) thefts, or the French response to Russian meddling in its elections.[45]

2.1.3 Step 3: Enhance the ability to detect and attribute

The last step in the Preparation Stage involves enhancing one's ability to detect a hybrid attack and attribute it to specific actors. From the outside, it is difficult to accurately evaluate how credible a state's ability to detect and attribute is. And while there are no international standards of proof for most of the retaliatory actions, countries still have a strong incentive not to make spurious allegations, lest they lose credibility. In addition, attribution is crucial as a lack

[38] Vincent A. Manzo, 'After the First Shots: Managing Escalation in Northeast Asia', *Joint Force Quarterly* 77, no. 2 (1 April 2015).

[39] Emilio Iasiello, 'Is Cyber Deterrence an Illusory Course of Action?', *Journal of Strategic Security* 7, no. 1 (March 2014): 54–67.

[40] Tim Sweijs and Samuel Zilincik, 'The Essence of Cross-Domain Deterrence', in *NL ARMS Netherlands Annual Review of Military Studies 2020*, ed. Tim Sweijs and Frans Osinga, NL ARMS (Springer), 129–58.

[41] David E. Sanger and Nicole Perlroth, 'U.S. Escalates Online Attacks on Russia's Power Grid - The New York Times', *New York Times*, 2019.

[42] European Commission, 'Commission Proposal for an Anti-Coercion Instrument', 2021.

[43] European Commission, 'EU Foreign Investment Screening Mechanism', 9 October 2020.

[44] Sweijs and Zilincik, 'The Essence of Cross-Domain Deterrence', 141.

[45] Louk Faesen et al., 'From Blurred Lines to Red Lines' (The Hague Center for Strategic Studies, 2020), 63–67.

thereof can create legal boundaries to possible countermeasures. Enhancing the ability to detect and attribute is especially pertinent for smaller states, such as the Netherlands, as it will increase their ability to rally support from third parties, attribute collectively and collaborate (e.g., through the EU or NATO). Overall, increasingly more states are engaged in public attribution, albeit with limited disclosure of the technical details of detection to preserve intelligence assets and techniques.

Increase detection capability

The ability to detect results from several components, comprising of international and inter-organisational cooperation, information sharing, analytical skills, technical expertise, and political willingness. At the outset, it involves collecting and analysing evidence from technical and other intelligence assets. This also requires an ability to connect various sources, both open and classified, across government agencies, to avoid stove piping of intelligence, and to see patterns and connect the dots across various manifestations of hybrid aggression. Based on the intelligence evaluation, the state will then make the political decision whether or not to communicate – openly or covertly – about the detection. Some states offer insights into their process, while others show off their capability through (counter-)intelligence operations.[46] Additionally, there can be an advantage to outsourcing the detection process to non-state actors to increase its credibility. However, it is unlikely that extreme measures (counter- and cyber-attack operations) can be argued with private sector detection alone. Most Western governments found that detection difficulties were an important barrier to deterring hybrid operations in cyberspace and the wider information environment. Consequently, they invested in increasing detection capabilities, which are typically accurate enough to allow retaliation with high confidence and legitimacy. However, it is also important to increase *collective* detection and attribution capabilities (e.g., through the EU or NATO) as this will improve the ability to act conjointly.

Strengthen ability to attribute within a politically meaningful timeframe

While it is possible to identify with varying degrees of certainty who is behind aggressive hybrid conduct, it might not be possible to attribute it in a politically meaningful timeframe, especially in conflict situations. Hence, defenders must strengthen their ability to attribute in a politically impactful timeframe, meaning that they must be able to attribute aggressive behaviour with sufficient confidence levels, either alone or as part of a broader alliance effort. To achieve this and justify a response, defenders must be willing to share potentially sensitive intelligence information, and following this, assess, evaluate and corroborate the gathered intelligence with allies.[47]

Prepare to convincingly explain attribution to third parties

In the hybrid domain, governments must often convince others that they are likely to know who misbehaved with sufficient confidence to enable retaliation. Communicating this ability can happen in several ways. They can, for example, openly disclose how their operational

[46] When the UK condemned Russia's GRU over a Georgia cyber-attack, a framework used by the UK government for all source assessments, including the probability yardstick, was published as well, albeit no longer publicly available. UK Government, 'UK Condemns Russia's GRU over Georgia Cyber-Attacks', 20 February 2020. It was also reported that the Netherlands intelligence service AIVD conducted an intelligence operation against Russian hacking Group Cozy Bear, which is associated with the GRU, and watched Russian hackers launch an offensive cyber operation against the US State Department. Rick Noack, 'The Dutch Were a Secret U.S. Ally in War against Russian Hackers, Local Media Reveal', *Washington Post*, 1 December 2021.

[47] Erica D. Borghard and Shawn W. Lonergan, 'Cyber Operations as Imperfect Tools of Escalation', *Strategic Studies Quarterly* 13, no. 3 (2019): 122–45.

intelligence collection and analysis functions work. However, very few governments voluntarily disclose this kind of information and there is a presumed extraordinary knowledge gap between the public (and even the 'knowledgeable public') and the intelligence reality. Instead, government attempts to protect their intelligence assets and techniques have led them to pursue other, less substantiated attribution methods. In short, a message of 'just trust us'. This, however, only works in favourable political circumstances and between trusted intelligence partners. Most leading liberal democracies have seen significant challenges to their credibility emerge over recent years. In 2018, the Dutch government was able to attribute the attempted hack of the Organisation for the Prohibition of Chemical Weapons (OPCW) effectively and quickly rallied support from like-minded countries, including the United Kingdom (UK) and the United States (U.S.).[48]

2.2 The Detection and Attribution Stage

The Detection and Attribution Stage focuses on the detection of hybrid attacks and the subsequent attribution of the attack to an opponent.

To ensure the detection of an incoming hybrid attack, one must make full use of the spectrum of resources available.

2.2.1 Step 4: Detect hybrid attack

Detect hybrid attack

To ensure the detection of an incoming hybrid attack, one must make full use of the spectrum of resources available, from international and inter-organisational cooperation to information sharing, analytical skills, technical expertise, and political willingness. Evidence must be collected and analysed using technical and other intelligence assets. In addition, collective detection capabilities should be employed through, for example, the EU and NATO, which can improve and extend the capabilities of its members. One can, subsequently, consider sharing the collected information with allies and partners to corroborate the intelligence findings. As stated before, intelligence can also be outsourced to non-state actors, which could positively benefit the credibility of findings.

2.2.2 Step 5: Consider attribution options

After the hybrid attack has been detected, a state must decide whether and the extent to which it will attribute. If attribution is chosen, defenders must attribute in a politically meaningful timeframe and explain the attribution convincingly to third parties in order to garner support.

Decide whether to attribute

Before deciding on the appropriate countermeasures to a hybrid attack, one must assess whether or not to attribute the detected attack. Attribution can help a state remove political or legal barriers to potential countermeasures by gathering support from larger segments of society and key allies. On the other hand, attribution exposes a state's intelligence assets

[48] Alicia Sanders-Zakre, 'Russia Charged With OPCW Hacking Attempt', Arms Control Association, November 2018.

and techniques, which it might want to protect. If attribution is the best course of action, states should consider covert and overt attribution. Through covert attribution, states could share their information with only a few selected partners. This would allow a state to garner support from key partners, enhance information sharing between allies, and potentially collaborate their response to said hybrid attack. Through public attribution, a state can gather support from larger segments of society and engage in naming and shaming. However, the extent to which details are disclosed should be assessed to preserve intelligence assets and techniques.

Attribute in an effective manner

If one decides to attribute, defenders must attribute in a politically meaningful timeframe and explain the attribution convincingly to third parties to garner support. First, states must attribute aggressive behaviour with sufficient confidence and supporting evidence, either alone or in conjunction with other parties. Smaller states, such as the Netherlands, should consider attribution as part of a broader alliance to strengthen the attribution effort. To attribute in a politically impactful timeframe, one must be willing to share potentially sensitive intelligence information with allies to justify any potential response as well as corroborate the intelligence through shared intelligence assessments. Second, attribution must be explained convincingly to third parties. This can be done by openly disclosing how a state's operational intelligence collection and analysis functions work. However, given the preservation and protection of their intelligence assets, few states have decided to disclose this. Instead, governments employ their political capital in the international community by stating to 'trust them'. This, however, only works in favourable political circumstances, and most leading liberal democracies have seen significant challenges to their credibility emerge over recent years.

Defenders must attribute in a politically meaningful timeframe.

2.3 The Decision-Making Stage

The Decision-Making Stage is pivotal in any successful counter-hybrid strategy. It is conveniently divided into three different steps that follow the preparation and detection stages: (i) choosing the response options, (ii) assessing the effectiveness of the response on the adversarial cost imposition, and (iii) evaluating the political willingness for and credibility of the countermeasure.

2.3.1 Step 6: Choose response options

The cross-domain character of hybrid conflict provides defenders with the opportunity to pick from a broad catalogue of alternatives across the DIMEFIL categorisation of instruments of state power, as well as to threaten asymmetrically. However, policymakers must assess the proportionality of available responses and anticipate their potential advantages and risks beforehan d (i.e., unwanted escalation, second- and third-order effects), as every countermeasure based on its unique characteristics will trigger both desired and undesired consequences.

Parse the available countermeasures across the DIMEFIL spectrum according to their impact

From a punishment perspective, deterrence in the hybrid domain extends beyond purely military retaliation to include measures from all instruments of state power. Given the cross-domain nature and effects of hybrid threats, symmetric responses are likely to prove ineffective or, to some extent, even detrimental. For instance, when dealing with disinformation, the decision to mirror the use of election meddling with in-kind responses is likely to erode democratic values, such as the freedom of elections or the freedom of information.[49] Similarly, the use of military operations to counter espionage and malicious cyber operations may constitute a blatant breach of international law, thus triggering escalation.[50] When it comes to economic coercion, in-band responses are likely to impact the broader globalised interconnectedness and even backfire against the deterrer and its allies.[51] As a final example, covert cyber operations, such as cyber intelligence (CNE), could easily be mistaken for cyber operational preparation of the environment (C-OPE) in view of a cyberattack. In contrast, operations carried out by third parties could be misattributed, thus provoking unwanted confrontations.[52] Therefore, to manage escalation horizontally and avoid triggering quick retaliation, defenders should elaborate a wise combination of overt and covert responses across domains in the hybrid environment.[53]

Deterrence in the hybrid domain extends beyond purely military retaliation to include measures from all instruments of state power.

Diplomatic

The diplomatic domain constitutes a 'dynamic and potent instrument'.[54] It includes measures – from demarches and bilateral channels to public attribution, naming and shaming tactics, diplomatic expulsions, and StratCom – intended to signal disapproval of the hostile's actions at the broader political level. While carrying the negligible risk of escalation, low-intensity diplomatic countermeasures have the advantage of fostering norm entrepreneurship at the international level, imposing social costs, and persuading hostile actors that their actions will likely be condemned on a widespread basis. In recent years, diplomatic responses involving public attribution of a conduct gained significant momentum within the EU and have, in some circumstances, proven successful.[55] Public attribution, as well as naming-and-shaming strategies, are a symbolic and effective tool to impose political costs on the adversary. For instance, the highly detailed Dutch attribution following the hacking of the OPCW, in tandem with the previously released details from the Skripal poisoning by the U.K., eventually led to a significant data breach of the identities of over 300 officers of the Main Directorate of the General Staff of Russian Armed Forces (GRU). At the same time, highly detailed public attribution or naming-and-shaming techniques may set a precedent and inevitably contribute to the adversary's narrative that a high-threshold burden of proof is always required by the victim to meaningfully attribute aggressive behaviours in the future.[56] In turn, diplomatic expulsion is

[49] Mikael Wigell, 'Democratic Deterrence: How to Dissuade Hybrid Interference', *The Washington Quarterly* 44, no. 1 (2 January 2021): 49–67.

[50] James A. Lewis, 'Cross-Domain Deterrence and Credible Threats' (Centre for Strategic & International Studies, July 2010).

[51] Jonathan Hackenbroich and Pawel Zerka, 'Measured Response: How to Design a European Instrument against Economic Coercion' (European Council on Foreign Relations, 23 June 2021).

[52] James M. Acton, 'Cyber Warfare & Inadvertent Escalation', *Daedalus* 149, no. 2 (2020): 133–49.

[53] Tim Sweijs et al., 'A Framework for Cross-Domain Strategies Against Hybrid Threats' (The Hague Center for Strategic Studies, 12 January 2021), 7.

[54] Sweijs et al., 27

[55] See, for instance, how the EU and US decided to overtly attribute the operations carried out by APT-28 between 2016 and 2018 to Russia: Jessica Haworth, 'Russian Hacking Group APT28 'Conducting Brute-Force Attacks' against Organizations Worldwide', The Daily Swig | Cybersecurity news and views, 2 July 2021.

[56] Louk Faesen et al., 'From Blurred Lines to Red Lines' (The Hague Center for Strategic Studies, 2020).

deemed the most coercive.[57] While an effective tool for damaging an aggressor's reputation, such a measure is likely to cause significant second-order effects, triggering rapid deterioration of the relations between states or escalatory responses by the adversary.[58] Furthermore, it may prove worthless in the face of opponents who strenuously reject allegations.

Economic and financial

The role of economic statecraft is becoming increasingly prominent in hybrid warfare.

The role of economic statecraft is becoming increasingly prominent in hybrid warfare. Economic countermeasures are offensive tools to assert influence and defensive means to counter aggression.[59] These measures include the threat or use of comprehensive sanctions, such as trade and financial sanctions (e.g., asset freezes, import/export bans, tariffs and duties, import/export controls, etc.), embargoes, foreign assistance reductions and cut-offs, as a foreign policy tool to alter the costs of a specific policy implemented by the adversary. Sanctions can also be directed against *countervalue* and *counterpolitical* targets, such as individuals or entities (so-called 'targeted' sanctions). However, the effectiveness of unilateral sanctions is highly dependent upon the specific constraints and legal mandate,[60] and should be consistent with international law. Furthermore, while unquestionably altering the cost-benefit calculus of the attacker, such overt coercive measures inevitably bear significant second-order effects, such as disruptive macroeconomic imbalances that could hit third parties, including allies,[61] as well as serious normative effects, such as the dismantlement of established legal principles governing trade cooperation and the weaponisation of multilateral institutions,[62] and serious humanitarian consequences.[63] It should also be noted that the balance of (economic) forces does not guarantee success. Among the wide spectrum of economic responses, financial sanctions, such as the freeze of the assets of a central bank, and unilateral trade sanctions, such as the impositions of countervailing duties embargoes, are deemed most coercive. Despite some egregious failures like the 60-year-long embargo on Cuba,[64] economic sanctions are increasingly used to threaten retaliatory consequences, and their deterrent value is highly debated.[65] For example, the West has imposed unprecedented

[57] In 2018, 19 EU member states and 10 other states, including the U.S., opted for expelling over 100 Russian diplomats in response to Russia's malicious cyber operations targeting the Organisation for the Prohibition of Chemical Weapons (OPCW) and the subsequent poisoning of Sergei Skripal. See Deutsche Welle, 'US Expels Russian Diplomats and Issues Sanctions over SolarWinds Hacking Attack | DW | 15.04.2021,' DW.COM, accessed April 29, 2022.

[58] Within the context of the 2018 malicious operations mentioned above, a significant deterioration of the relationship between Russia and the U.S. was the ultimate result of the determination to expel Russian diplomats, as Russia retaliated by expelling, in turn, 40 American diplomats and closing the American Consulate in St. Petersburg. See Andrew Higgins, 'Expelling Diplomats, a Furious Kremlin Escalates a Crisis', *The New York Times*, 29 March 2018, sec. World.

[59] Rafał Wiśniewski, 'Economic Sanctions as a Tool of China's Hybrid Strategies', *Polish Political Science Yearbook* 50, no. 1 (31 December 2021): 1–13.

[60] As opposed to the US, the EU has always maintained that the extraterritorial application of unilateral sanctions is not consistent with international law and it has expressed its will to abide by such rules; see, European Commission, 'Communication: The European Economic and Financial System: Fostering Openness, Strength and Resilience', 19 January 2021.

[61] For instance, in response to the alleged use of unfair trade practices, the US have deployed a massive set of economic sanctions against China, including a vast array of trade retaliatory measures in blatant contrast with the rules set by the General Agreement on Tariffs and Trade (GATT). Such measures not only produced detrimental effects on both US and Chinese economies, but had significant implications for several other states. See Davin Chor and Bingjing Li, 'The Impact of the US-China Tariff War on China's Economy: New Evidence from Night-Time Lights', *VoxEU.Org* (blog), 25 November 2021.

[62] Elvire Fabry and Erik Tate, 'Saving the WTO Appellate Body or Returning to the Wild West of Trade?' (Jaccques Delors Institute, 7 June 2018).

[63] Mohamed M. Ali and Iqbal H. Shah, 'Sanctions and Childhood Mortality in Iraq', *The Lancet* 355, no. 9218 (27 May 2000): 1851–57.

[64] Isabella Oliver and Mariakarla N. Venancio, 'Understanding the Failure of the U.S. Embargo on Cuba' (WOLA, 2022).

[65] Dursun Peksen, 'When Do Imposed Economic Sanctions Work? A Critical Review of the Sanctions Effectiveness Literature', *Defence and Peace Economics* 30, no. 6 (19 September 2019): 635–47.

economic sanctions on Russia following its invasion of Ukraine in 2022 but has thus far failed to deter Russia. The continued export of Russian gas to the EU and continued trade between Russia and non-Western countries, including China, India, and South Africa, have softened the blow of economic sanctions and reduced their effectiveness.[66] Similarly, the imposition by the EU of targeted sanctions – including travel bans and the freezing of assets – on six individuals and three entities involved in various Russia-linked cyber-attacks against legislative bodies and other public institutions in member states have not achieved the expected results from a deterrence perspective.[67]

Information and Intelligence

The information domain, through its systems and networks, may be exploited to pursue aggressive objectives (e.g., disinformation, election meddling, and cyber operations)[68] as well as for the purposes of policy and deterrence. Threatening retaliation with covert countermeasures, so as to discourage changes in an adversary's policy, can be achieved through system intelligence and information operations. Here, information on the adversaries' capabilities is gathered and ideally communicated to the adversary with the threat of retaliatory cost imposition or attribution. The same objective may also be achieved through counterintelligence, which entails detecting, monitoring, and foiling the target's attempts to gather intelligence on one's assets (military, diplomatic, economic, information) by using human intelligence, signals, and electronic intelligence. While intelligence operations are unlikely to cause any normative or second-order effects because they are not prohibited under international law and do not establish precedents, counterintelligence may be prone to escalate quickly if it is unmasked by the adversary.[69]

Deterrence can also be achieved using cyberspace through four main tactics, all of which must adhere to international law. Firstly, *offensive counter cyber operations* may be used to target a botnet server, which forces a country to shut down all non-essential Internet traffic, or to insert malware against adversarial military infrastructure, such as the telecommunications system. Secondly, *cyber support operations*, which include cyber and electromagnetic activities or counter-information warfare activities, may be used to target terrorist recruitment and propaganda efforts. Thirdly, *cyberattacks* may be carried out at both tactical and strategic levels, targeting both counterforce targets, such as adversarial command and control structures, and countervalue targets, such as power grids, petrochemical plants, energy systems, water dams, and gas pipelines. Lastly, *counter cyber disinformation campaigns* may be utilised, which include debunking, the use of elves, StratCom, norm setting, and even shutting down media operations of an opponent.[70] For instance, during the attempted Russian meddling in the French elections, the team of French President Macron decided to communicate openly and extensively about the hacking and disinformation operations, gained control over

[66] Tim Sweijs and Mattia Bertolini, 'How Wars End: War Terminations: Insights for the Russia-Ukraine War' (The Hague Center for Strategic Studies, May 2022), 9.

[67] European External Action Service, 'EU Imposes First Ever Cyber Sanctions to Protect Itself from Cyber-Attacks', 30 July 2020.

[68] Kevin Pollpeter, 'Controlling the Information Domain: Space, Cyber, and Electronic Warfare', in *Strategic Asia 2012-13: China's Military Challenge*, ed. Ashley Tellis and Travis Tanner (The National Bureau of Asian Research, 2012), 162–94.

[69] Sweijs et al., 'A Framework for Cross-Domain Strategies Against Hybrid Threats'.

[70] In 2019, as part of *Operation Synthetic Theology* to safeguard midterm elections, the U.S. CYBERCOM not only hacked and shutdown the Russian Internet Research Agency, but it also disclosed it had pre-deployed cyberweapons within Russian critical infrastructures in order to strike a kinetic-equivalent attack, if necessary. The U.S. coercive assertion in cyberspace against Russia bears significant normative effects, as it is broadly considered a violation of the customary principle of non-intervention; For countering disinformation, see Faesen et al., 'From Blurred Lines to Red Lines', 2020; Louk Faesen et al., 'Red Lines & Baselines: Towards a European Multistakeholder Approach to Counter Disinformation' (The Hague: The Hague Center for Strategic Studies, October 2021).

the leaked information through forged emails that they placed in Honeypots, and actively debunked disinformation on social media. These debunking initiatives were not isolated to the Macron campaign team but collated around several independent research projects and reliable media sources who fact-checked the rumours levelled at Macron, mainly from his opponent Marine Le Pen.

Military

Measures in the military domain can be conducted across land, sea, air, cyberspace, and space. Distinguishing between military and non-military efforts in the context of hybrid deterrence may frustrate the defender's capability to protect its core interests from foreign aggression. However, the military is undoubtedly the domain that offers responses most likely to trigger vertical escalation. Hence, while still being an essential pillar of deterrence, military efforts in the hybrid domain should be significantly calibrated to avoid unintended consequences. Military responses span from counter-cyber operations and cyber-attacks,[71] port visits,[72] defence attaché networks,[73] Freedom of Navigation Operations (FONOPS), and military exercises (including special forces operations). Deterrent effects may be achieved by credibly establishing retaliatory – ideally overwhelming – military capabilities, and by communicating it accordingly. However, this strategy ultimately relies on the competitive advantage that big powers wield.[74] Yet, in the hybrid domain, military activities extend beyond traditional field operations to include psychological operations (PsyOps) and information manoeuvres, although these have legal boundaries. Psychological operations, which the U.S. doctrine divides into strategic, operational, and tactical PsyOps, can be used to 'convey selected information and indicators to foreign audiences to influence their emotions, motives, objective reasoning, and ultimately the behaviour of foreign governments, organisations, groups, and individuals.'[75] Psychological operations are a low-intensity tool to combine persuasive narratives with credible threats to fuel discontent, undermine foreign leaderships, and degrade the actual capability to sustain an adversary's ability to conduct or support military operations. For instance, to counter the massive propaganda carried out by the Islamic State (IS), the U.K. sent daily media packages covering IS' atrocities and recommending StratCom countermeasures to upskill countries with less communications experience. These initiatives focused on a fact-based refutation of the IS narrative, undermining their image as victors by propagating the message that they were losing on the ground and failing to present a positive vision for the region.[76]

Legal

The legal domain, at both international and domestic levels, may provide effective tools for countering hybrid threats, spanning from criminal prosecution and indictments to the establishment of landmark proceedings before international courts and tribunals, and the

[71] Ken Dilanian and Courtney Kube, 'Biden given Options for Unprecedented Cyberattacks against Russia', *NBC News*, 24 February 2022.

[72] Jukka Savolainen et al., *Handbook on Maritime Hybrid Threats: 10 Scenarios and Legal Scans: Working Paper*, ed. Tiia Lohela and Valentin J. Schatz (Helsinki: European Centre of Excellence for Countering Hybrid Threats, 2019), 29.

[73] Ministry of Defence, 'Defence Secretary Sir Michael Fallon Hails Importance of UK's Defence Network' (UK Government, 10 January 2017).

[74] Roger McDermott, 'The Kremlin's Strategy on Ukraine and Conflict De-Escalation', *The Jamestown Foundation - Eurasia Daily Monitor* (blog), 29 April 2014.

[75] Steven Aftergood, 'DoD "Clarifies" Doctrine on Psychological Operations', *Federation Of American Scientists* (blog), 19 January 2010.

[76] Dan Chugg, 'Winning the Strategic Communications War with Daesh - Civil Service Quarterly', *Civil Service Quarterly* (blog), 20 December 2017.

negotiation of new treaties.[77] The legal domain offers subtle but valuable deterrence tools which are unlikely to trigger direct escalation. On the one hand, domestic rules and enforcement mechanisms can be creatively modelled to perform covert intelligence operations, to covertly and implicitly set thresholds, and to signal the will to protect a specific interest from aggressive foreign behaviours in the grey zone. For example, Finland was able to gather significant intelligence information about Russian real estate investments in its territory by creatively performing anti-money laundering and tax proceedings. It then resorted to norm development and introduced new limits on foreign direct investments in the real estate sector without publicly declaring that Russian investments constituted aggressive influence (redline) nor overtly signalling its will to punish such behaviours.[78] More overtly restrictive legislation has been adopted by France in the aftermath of Russian interference attempts during Macron's 2017 election campaign. As a result, a judge may be requested to order the immediate removal of alleged fake news spread on media platforms with the aim of preventing the manipulation of digital information.[79] Similarly, legal instruments can be used to expand a country or organisation's legal basis and to lift existing restraints to counter-hybrid threats.[80] Interestingly, while having routinely criticised the use of unilateral (extraterritorial) sanctions as inconsistent with international law, the EU is in the process of establishing regulation designed to protect the Union from economic coercion. The regulation covers a wide spectrum of responses to counter foreign economic interference, spanning from the least coercive (such as diplomatic engagement with the third country concerned) to the most coercive ones (such as unilateral sanctions).

The legal domain, at both international and domestic levels, may provide effective tools for countering hybrid threats.

Moreover, indictments have been routinely used by the U.S. against members of state-sponsored cyber groups,[81] as well as independent criminals involved in election interference. Recently, German prosecutors have issued a warrant for the arrest of a Russian national linked to the Federal Security Service (FSB) and allegedly involved in a cyber-attack on a German electricity company back in 2017.[82] While signalling a strong will to punish, indictments may prove ineffective due to the frequent failure by states to successfully carry out extradition procedures or due to the impossibility of effectively tracking and bringing suspected persons to trial. Even more so, recent experience demonstrates that indictments can be counterproductive. For instance, it has been reported that, while facing trial within the context of the alleged Russian interference in the 2016 presidential elections, Russian firm Concord '[...] seized on the case to obtain confidential information from the prosecutors' in order to subsequently mount an information warfare campaign and ultimately weaponise the criminal trial as a response to election meddling.[83]

As recent events demonstrate, the legal domain may also be used as a tool to exert control through pre-emption at the international level, by withdrawing from or even instrumentalising

[77] John Sakellariadis, 'How the Justice Department Is Stepping up Its Efforts To Indict State-Sponsored Hackers,' *The Record by Recorded Future* (blog), February 3, 2021.

[78] Rachel Ellehuus, 'Strange Birds in the Archipelago: Finland's Legislation on Foreign Real Estate Investment', Center for Strategic & International Studies, *Kremlin Plabook Spotlight* (blog), 7 April 2020.

[79] Irène Couzigou, 'The French Legislation Against Digital Information Manipulation in Electoral Campaigns: A Scope Limited by Freedom of Expression', *Election Law Journal: Rules, Politics, and Policy* 20, no. 1 (March 2021): 98–115.

[80] See European Commission, 'EU Strengthens Protection against Economic Coercion', European Commission, 8 December 2021.

[81] Bill Chappell and Carrie Johnson, 'U.S. Charges 7 Russian Intelligence Officers With Hacking 40 Sports And Doping Groups', *NPR*, 4 October 2018, sec. Europe.

[82] Jonathan Greig, 'German Prosecutors Issue Warrant for Russian Government Hacker over Energy Sector Attacks', *The Record by Recorded Future* (blog), 29 July 2022.

[83] See Katie Benner and Sharon LaFraniere, 'Justice Dept. Moves to Drop Charges Against Russian Firms Filed by Mueller', *The New York Times*, 16 March 2020, sec. U.S..

a multilateral treaty. This is what the U.S. ultimately attempted to do in the broader context of its trade war against China once it became clear that the imposition of sanctions would not generate the desired effects against Chinese coercive practices as China had challenged these measures before the World Trade Organisation (WTO). Indeed, as a last resort, the U.S. decided to strategically block the dispute settlement body of the WTO by halting the appointment of new nominees.[84] However, instrumentalising international *fora* ultimately undermines the political will of other states to adhere to established and shared international norms, thus carrying significant second- and third-order effects.

In summary, the DIMEFIL spectrum offers a wide range of responses to craft cross-domain strategies against hybrid threats. However, such rich variety comes with clear warnings and risks due to the ambiguities and entanglements that characterise hybrid operations. To respond asymmetrically and avoid escalation and undesired effects, policymakers must develop a comprehensive framework that links activities and correspondent effects across domains. [85] This allows a state to identify the costs of specific actions and facilitates the selection of the most appropriate response to counter-hybrid threats. When parsing countermeasures, defenders must identify targets, assess the inherent characteristics of countermeasures, manage proportionality and escalation, as well as potential second- and third-order effects, not only across domains and theatres but also across allies and partners.[86]

Identify possible targets across multiple domains, including counterforce, countervalue, and counterpolitical targets

Possible targets must be identified across three domains: *counterforce*, *countervalue*, and *counterpolitical* targets. Counterforce targets are traditionally associated with military assets, with the aim of hitting and degrading the opponent's technical capability. On the other hand, countervalue targets are not associated with the military but comprise strategically significant civilian assets, such as energy and health infrastructures, and financial institutions. Therefore, countermeasures against countervalue targets have a wider economic and societal impact. Lastly, counterpolitical targets are assets pertaining to specific individuals or entities with critical political value and exert psychological influence on a country, regardless of that value being widely known by the public. Despite being clearly distinguished at the conceptual level, in reality the three categories described can partly overlap, with one target potentially being relevant as a counterforce, countervalue, and counterpolitical. The interconnectedness of these target types must therefore be considered when deciding on responses in the hybrid environment. Additionally, a vulnerability assessment of the opponent should be conducted to identify where the actor can successfully be targeted.

Assess the legality of the response options

The legality of each response option should be assessed carefully. Potential countermeasures should be adopted by national and international law. This way, potential legal boundaries to the chosen course of action are removed or significantly lowered. Moreover, increasing the legality of a counter-hybrid response can greatly increase its effectiveness. For example, as mentioned above, the success of unilateral sanctions can depend on the legal mandate within

[84] AJIL, 'United States Continues to Block New Appellate Body Members for the World Trade Organization, Risking the Collapse of the Appellate Process', *American Journal of International Law* 113, no. 4 (October 2019): 822–31.

[85] Sweijs et al., 'A Framework for Cross-Domain Strategies Against Hybrid Threats', 24.

[86] Jim Garamone, 'Concept of Integrated Deterrence Will Be Key to National Defense Strategy, DOD Official Sa', U.S. Department of Defense, 8 December 2021.

which they operate. Small- and medium-sized powers, such as the Netherlands, should be mindful of the legal permissibility of their chosen response options as their countermeasures should be conducted with the support of like-minded partners and operated within broader international legal frameworks.

Assess the duration and the timeframe within which they come into effect

It is crucial to evaluate beforehand whether responses produce immediate or long-term effects and whether their effects are temporary or permanent. For instance, retaliatory actions through cyberspace cannot be undone once unleashed. Consequently, should specific conduct be misattributed to the target actor, cyber responses are likely to trigger escalation and undermine the general confidence in cyberspace hygiene. On the contrary, responses in other domains, such as economic sanctions, can easily be rolled back and their effects interrupted. However, sanctions' tangible effects can normally be appraised in the long term, thus requiring strategic patience. While this allows policymakers to evaluate their overall effects, including second- and third-order effects, more calmly, such measures are unlikely to be perceived as a serious deterrer threat, unless their magnitude constitutes an existential threat to the economic survival of the targeted state.

The legality of each response option should be assessed carefully.

Consider the proportionality of the countermeasure

Responses against hybrid conducts should maintain proportionality, to avoid immediate escalation or setting precedents for escalatory responses in peacetime. A response is proportionate to the extent that it does not represent an *existential threat* or futile provocation to the aggressor. While inherently a subjective metric, proportionality can be framed as a function of intersubjective proportionality. In turn, this can be framed as a function of instruments deployed – which relates to the character of the domains in which the measure operates – and the effects achieved – which could be divided into context most measures are likely to produce the impact of both types. A failure to undertake a proportionality assessment is expected to result in unintended escalation, prompting what the defender was aiming to deter in the first place.[87]

The U.S. decision to impose economic sanctions on Russia in response to the interference in the 2016 presidential elections is an example of a disproportional asymmetric response, as it also affected U.S. partners. The Countering America's Adversaries Through Sanctions Act targeted any moral or physical person that 'contributes to the Russian energy export pipelines, goods, services, technology, information, or support' by limiting their access to U.S. financial means. In doing so, U.S. measures eventually ended up affecting EU companies that were lawfully carrying out investments in the Russian energy sector.[88] U.S. economic retaliation was characterised by an apparent lack of proportionality, which inevitably brought about a significant risk of escalation, and the potential degradation of relations with key partners due to the dismissive attitude towards their interests. In this regard, several EU member states immediately underlined the disproportionate and unreasonable character of such countermeasures by reiterating that sanctions against Russia should not become a tool of industrial policy to pursue U.S. interests. From a normative perspective, the EU also countered U.S. efforts by clearly signalling the illegality of the extraterritorial application of sanctions.[89]

[87] Stephanie Pezard and Ashley L. Rhoades, 'What Provokes Putin's Russia?: Deterring Without Unintended Escalation' (RAND Corporation, 29 January 2020).

[88] Eyes on Europe, 'How the EU should respond to the new US sanctions against Russia?' *Eyes on Europe* (blog), August 23, 2017.

[89] European Parliament, 'Answer given by Vice-President Borrell on Behalf of the European Commission', European Parliament, 4 February 2020.

Identify entanglements and second- and third-order effects

Countermeasures can be distinguished between overt and covert ones. Overt countermeasures, such as indictments, unilateral sanctions, diplomatic expulsion, military intervention, and cyber-attacks, are more likely – although not necessarily – to trigger third-order and normative effects, and set precedents for escalatory responses in peacetime, which may lead to direct tit-for-tat escalation. In contrast, covert responses, such as the U.S. doctrine of persistent engagement in cyberspace, traditionally rely on a wider legal mandate and produce limited third-order and normative effects.[90] However, they inevitably prove less effective from a deterrence perspective. Adverse effects when crafting responses to hybrid threats are often disregarded or underestimated. However, they significantly cripple the long-term effectiveness of deterrence and eventually backfire. Relevant examples of such unintended and detrimental consequences may be drawn from the use of kinetic cyber operations to counter disinformation.[91] While serving as an effective means to penetrate adversaries' networks, using offensive cyber means against state actors inevitably bears the risk of weaponising the information environment and mass media, and is likely to undermine existing norms in a way that eventually supports the opponent's interpretation.[92] Similarly, the use of overt countermeasures, such as indictments and economic sanctions, to respond to industrial espionage may escalate lawfare and reduce international cooperation in critical sectors.[93] However, the use of offensive cyber capabilities has proven successful against non-state actors, as in the case of the major offensive cyber campaign carried out by the U.K. against the Islamic State.[94]

Conduct an escalation assessment

Assessing the risk of a potential escalation in relation to countermeasures is complicated by the issues discussed about attribution, signalling and proportionality. Before the actual execution of a countermeasure, it is rather difficult to anticipate the effects it is likely to produce in the cross-domain context. This is mostly due to (i) a lack of clear understanding of what constitutes a proportional threat, given the absence of a shared framework to help policymakers; (ii) the inherent characteristics of the tools and weapons used in the hybrid context, as well as their cross-domain effects, which inevitably destabilise rational decision-making; (iii) the fact that different actors have different subjective perceptions regarding courses of action and attach different significance to the interaction between different domains.

Although it is a difficult task, assessing the risk of escalation is crucial to the design of counter-hybrid postures. In the hybrid context, escalation management is a practical exercise, varying from context to context. As a general rule of thumb, cross-domain entanglements spontaneously create mutual dependencies and vulnerabilities, thus providing states with an incentive to act cautiously. Then, defenders should channel competition into clear patterns by taking advantage of norm entrepreneurship at the international level. Setting up a framework with broad thresholds that are shared among the international community reduces ambiguity

[90] United States Cyber Command, 'Achieve and Maintain Cyberspace Superiority: Command Vision for US Cyber Command' (National Security Archive, 23 March 2018).

[91] Ellen Nakashima, 'U.S. Cyber Command Operation Disrupted Internet Access of Russian Troll Factory on Day of 2018 Midterms', *Washington Post*, 27 February 2019.

[92] Alexander Klimburg, 'Mixed Signals: A Flawed Approach to Cyber Deterrence', *Global Politics and Strategy* 62, no. 1 (2 January 2020): 107–30.

[93] Lorand Laskai and Adam Segal, 'A New Old Threat: Countering the Return of Chinese Industrial Cyber Espionage', Digital and Cyberspace Policy Program (Council on Foreign Relations, 6 December 2018).

[94] BBC, 'UK Launched Cyber-Attack on Islamic State', *BBC News*, 12 April 2018, sec. Technology.

and leads to a mutual understanding of what constitutes proportionality and what is likely to trigger escalation. Finally, from a practical perspective, defenders should avoid using specific 'weapons' against specific 'targets'. For instance, it is rather straightforward that the threat of nuclear retaliation against C2 structures will likely trigger quick vertical escalation. In the information domain, responding to disinformation with more disinformation inevitably weaponises the use of media and generates mistrust in public information. Considering the economic domain, it is reasonable to expect that using the most severe financial and trade sanctions, such as the freeze of central banks or embargoes, will likely trigger escalation and undermine norm adherence.

> Assessing the risk of escalation is crucial to the design of counter-hybrid postures.

Table 2: Cross-domain countermeasures, their targets, and second-order effects

Domain	Countermeasure	Target	Second-order effects
Diplomatic	Diplomatic expulsions	n/a	Fraying diplomatic relations
	Naming and shaming tactics	State, Countervalue, counterpolitical	Lack of clarity regarding the incident undermines credibility and favours escalation
	Public attribution	State, Countervalue, counterpolitical	The more attribution is detailed, the higher the burden of proof required in the future to meaningfully attribute
	Public diplomacy	n/a	n/a
	Demarches	n/a	n/a
Information and intelligence	Offensive Counterintelligence	Counterforce, Counterpolitical, Countervalue	Risk of escalation
	System intelligence	Counterforce, Counterpolitical, Countervalue	n/a
	Cyber support operations (civilian)		
	Information Operations (InfoOps)	Counterforce, Countervalue	
	Strategic Communication (StratCom)	Countervalue, Counterpolitical	n/a

Table 2: Cross-domain countermeasures, their targets, and second-order effects (continued)

Domain	Countermeasure	Target	Second-order effects
Military	Offensive cyber operations and cyber-attacks	Counterforce, countervalue	Weaponisation of information, misunderstanding, misattribution, escalation
	Cyber Electromagnetic Activities (CEMA)	Counterforce, countervalue	
	Military exercises	n/a	Potential instability, provocation, escalation
	Port visits	Counterforce, countervalue	
	Defence attaché networks	n/a	n/a
	Psychological Operations (PsyOps)	Countervalue, Counterforce, Counterpolitical	Mistrust in the information environment
	Military Deception (MILDEC)	Counterforce	
	Freedom of Navigation Operations (FONOPs)	Counterforce, countervalue	Unintended escalation
Economic and financial	Freeze of the assets of a central bank	Countervalue	Escalation, humanitarian consequences
	Embargoes	Countervalue	Economic warfare, norm adherence reduction, humanitarian consequences
	Tariffs and duties	State, Countervalue	Potential macroeconomic backfire, norm adherence reduction
	Import/export bans	State, Countervalue	Norm adherence reduction
	Import/export controls	State, Countervalue	Norm adherence reduction
	Individual targeted sanctions	Countervalue, counterpolitical	
	Foreign assistance reductions and cut-offs	State	
Legal	Criminal prosecution and indictments	Countervalue, counterpolitical	Lawfare escalation
	Establishment proceedings before international courts and tribunals	State, Countervalue, Counterpolitical	Political unwillingness to enforce rulings
	Domestic law enforcement mechanisms	Countervalue, counterpolitical	
	Norm development	n/a	n/a

2.3.2 Step 7: Assess effectiveness of response on adversarial cost-imposition perception

In the third stage, policymakers must evaluate and assess whether the measures will likely affect the cost-benefit calculus of the specific aggressor one aims to deter and, thus, change the opponent's behaviour. Counter-hybrid postures centred on active deterrence can only be successful if the defender can impose psychological, political, or material costs on the adversary without incurring undesired effects and triggering escalation. Responses should adequately consider what motivates hybrid actors by exploring their domestic and international support and investigating entanglements, vulnerabilities, and dependencies to parse the measures most likely to affect its cost-benefit calculus and ultimately deter it.

Examine costs at the psychological level

In the hybrid context, where responses are asymmetrical and span across different domains to exploit entanglements, the effectiveness of responses carried out through the DIMEFIL spectrum should be tested against the real-world motivations and core interests of the adversary, its propensity for offence,[95] as well as the vulnerabilities that the latter aims to shield from possible retaliation.[96] 'Who' is the opponent, really? Traditional deterrence literature suggests that '[...] strategies must aim to influence cost-benefit calculations by specific leaders, not generic states'.[97] However, hybrid threats add significant layers of complexity in this regard. On the one hand, it is not always a sovereign state led by a specific leader that carries out aggressive and influential operations but rather individuals, groups, and other non-state actors with direct or indirect links to a foreign government. On the other hand, cross-domain responses incentivise aggressors to find solutions to circumvent and frustrate a target's defence by simply relocating the threat to a different domain.[98]

Aggressors', either state or non-state entities, resolve to threaten or attack is based on several factors and specific motives. Such resolve is seldom grounded on rational decision-making and, as Patrick Morgan notes, 'the intentions of opponents are notoriously difficult to fathom'.[99] History shows that an aggressor would unlikely be deterred whenever it sees that attacking is the only way to safeguard its interests.[100] It is commonly accepted that ideologically motivated leaders are more risk tolerant and less likely to step back when facing the threat of punishment.[101] Identifying an adversary's vulnerabilities is further complicated by the current interconnectedness and by the fact that opponents are rarely isolated, either diplomatically, militarily or economically. In some cases, hostile states may even welcome

[95] Michael J. Mazarr, 'Understanding Deterrence' (RAND Corporation, 19 April 2018).

[96] Michael Ruhle, 'The Nine Commandments on Countering Hybrid Threats | Internationale Politik Quarterly', Internationale Politik Quarterly, 22 April 2021.

[97] Michael J. Mazarr et al., 'What Deters and Why: Exploring Requirements for Effective Deterrence of Interstate Aggression' (RAND Corporation, 20 November 2018), 12.

[98] For instance, when the US resorted to overt offensive cyber operations to hack Russian systems and counter influence operations, Russia shifted asymmetrically by sponsoring cyber criminals using ransomware and other cyber-attacks. This is in part possibly because of their very vast web of non-state proxies that are loosely governed. See Joe Tidy, '74% of Ransomware Revenue Goes to Russia-Linked Hackers', *BBC News*, 14 February 2022, sec. Technology.

[99] Patrick M. Morgan, *Deterrence Now*, Cambridge Studies in International Relations (Cambridge: Cambridge University Press, 2003), 39.

[100] During World War II, despite being aware of the high risk of losing a long war, Japan felt that economic manoeuvres carried out by the U.S. and the UK were severely undermining its imperial vocation. Hence, when deciding to go to war, Japan felt utterly motivated, despite a rational decision-making analysis of the actual circumstances would have suggested to abstain.

[101] Shmuel Bar, 'God, Nations, and Deterrence: The Impact of Religion on Deterrence', *Comparative Strategy* 30, no. 5 (14 December 2011): 428–52.

retaliation, as it provides the political justification for expanding their sphere of action.[102] The involvement of non-state actors also undermines the effectiveness of several countermeasures because, unlike states, they rarely possess assets to freeze and are mostly indifferent to diplomatic discourses.[103]

The starting point is that adversaries may be more or less prone to act and accept the risk of retaliation depending on various psychological components. This means that the likelihood of them being deterred ultimately rests on how closely they value their strategic goals and how credibly they believe that the defender would retaliate. While it would be virtually impossible to identify with certainty what exactly moves an adversary, an in-depth analysis of the aggressor's motivations, historical behaviour, and current leadership still allows defenders to build wargame scenarios that reflect different degrees of risk-propensity and to craft a menu of meaningful cross-domain responses.[104] Cognitive modelling plays a crucial role in anticipating how an adversary might behave and perceive the threats signalled by the defender. Setting up different behavioural models for the same adversary also prevents defenders from incurring cognitive biases and misunderstandings, such as mirror-imaging, stereotyping, overestimating one's capabilities, and the tyranny of the best estimate.

Examine costs at the political level

The diversionary theory of war suggests that a state's domestic policies largely shape foreign politics.[105] As Jack Levy notes, '[...] political elites often embark on adventurous foreign policies or even resort to war to distract popular attention away from internal social or economic problems and consolidate their own domestic political support'.[106] In the first regard, a counter-hybrid strategy must aim to cripple domestic support for the opponent's leadership by identifying and targeting 'internal or domestic groups whose support is required for the continued functioning of the state or non-state organisation'.[107] Unilateral targeted sanctions against *counterpolitical* targets, such as oligarchs or companies with high intrinsic and symbolic value within a country, may be useful in undercutting domestic support.[108] However, the effectiveness of such measures is utterly dependent on the adversary's socio-economic context and the degree of control that the government can exert on the wider society. For instance, it has been observed that the decision to 'freeze' rather than 'seize' Russian oligarchs' assets, although consistent with legal restraints that guide Western legal systems, has routinely proved ineffective in crippling Putin's domestic support.[109]

[102] Lyle Morris et al., *Gaining Competitive Advantage in the Gray Zone: Response Options for Coercive Aggression Below the Threshold of Major War* (RAND Corporation, 2019).

[103] Lewis, 'Cross-Domain Deterrence and Credible Threats'.

[104] Paul K. Davis et al., 'Influencing Adversary States: Quelling Perfect Storms' (RAND Corporation, 16 February 2021). The Authors develop a wargame scenario based on three different cognitive models for the same adversary.

[105] Joe D. Hagan, 'Diversionary Theory of War in Foreign Policy Analysis', Oxford Research Encyclopedia of Politics, 26 October 2017.

[106] Jack S. Levy, 'The Diversionary Theory of War: A Critique'. Handbook of War Studies (ed. Manus I. Midlarsky) (1989), 269.

[107] Gary Schaub, 'When Is Deterrence Necessary? Gauging Adversary Intent', *Strategic Studies Quarterly* 3 (1 January 2009): 27.

[108] Paul Massaro, The effects of sanctions targeting Russian oligarchs, interview by Michel Martin, NPR, 6 March 2022.

[109] The role and effectiveness of recent sanctions enacted against Russian oligarchs in the context of the invasion of Ukraine has been downplayed by some observers for several reasons.: see Sam Tabahriti, 'Oligarch Sanctions Were Essentially a Good Idea but They Won't Sway Putin — and the Aftermath Is Uncertain, Says Expert', Business Insider, 3 April 2022.

Instead of seizing *countervalue* and *counterpolitical* targets, defenders can undermine an adversary's political legitimacy by engaging in advanced operations to unveil propaganda and cover-ups orchestrated by authoritarian regimes or terrorist groups, and use that as bargaining leverage in future negotiations.[110] For instance, several countries have reportedly used offensive cyber capabilities to counter IS propaganda and degrade the terrorist's credibility and 'attractiveness'.[111] Similarly, the EU has established the East StratCom Task Force to counter Russian influence efforts targeting eastern European states.[112]

At the international level, defenders must aim to curtail international acquiescence, support, and cooperation with the target by calibrating narratives based on shared values and principles. For instance, to de-legitimise an aggressor engaging in election meddling, it is more effective to portray such behaviour as starkly in contrast with every state's fundamental right to sovereignty, instead of pushing forward narratives based on the ideological contraposition between democratic and autocratic values. Diplomatic efforts through naming and shaming techniques and stigmatisation, as well as the creation of collective defence mechanisms based upon diplomacy,[113] also constitute a valuable way to project soft power[114] to boost transparency, destabilise and isolate an adversary at the global or regional stage, and to promote the emergence of new norms.[115]

Examine costs at the economic and operational level

Imposing economic and operational costs in the hybrid domain is traditionally achieved through the imposition of comprehensive sanctions, and targeted sanctions implemented against countervalue targets, such as corporations operating in strategic sectors and financial institutions. In general, sanctions can restrict access to markets and resources used to fuel aggressive operations. Such measures also induce discontent across the wider society, which can be strategically leveraged to undermine a leader's domestic support. However, this is where the sore point lies: indeed, the potential impact of sanctions on the broader society still constitutes the 'central problem of both comprehensive and targeted sanctions.'[116]

Whether economic countermeasures ultimately work or not rests on several factors.

Whether economic countermeasures ultimately work or not rests on several factors that are extremely difficult to assess. In this regard, a target may easily circumvent comprehensive trade sanctions by gaining access to alternative markets, acquiring resources from other partners operating in the current globalised system, or substituting restricted foreign goods with domestic production (where possible). All such variables should be thoroughly anticipated and understood, as economic countermeasures have routinely been considered counterproductive. Indeed, a comprehensive empirical study on the effectiveness of economic sanctions found that, in general, such measures were effective only in 34% of the cases.[117] When narrowing down to the circumstances in which sanctions were used to destabilise leaders or push autocratic governments to democracy, the rate drops to a discouraging 25%. For example, asset freezes and other economic restrictions imposed against Russian banks

[110] Wigell, 'Democratic Deterrence', 61.

[111] See, BBC, 'UK Launched Cyber-Attack on Islamic State', *BBC News*, 12 April 2018, sec. Technology.

[112] Strategic Communications, '2021 StratCom Activity Report - Strategic Communication Task Forces and Information Analysis Division', European External Action Service, 24 March 2022.

[113] NATO, 'Collective Defence - Article 5', NATO, accessed 9 June 2022.

[114] Joseph S. Nye, 'Soft Power', *Foreign Policy* 80 (1990): 153–71.

[115] Faesen et al., 'From Blurred Lines to Red Lines', 2020.

[116] Francesco Giumelli, 'Targeted Sanctions and Deterrence in the Twenty-First Century', 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, NL ARMS (The Hague: T.M.C. Asser Press, 2021), 350.

[117] Richard N. Haass, 'Economic Sanctions: Too Much of a Bad Thing', *Brookings* (blog), 1 June 1998.

and financial operators in the aftermath of the annexation of Crimea were aimed at crippling the Russian economy in crucial sectors. However, the strategy to impose costs at the economic level did not play out as intended due to the target's readiness to endure, forged by significantly depleting sovereign funds, which slashed the state budget to provide emergency capital to banks, and avoiding the rouble from plummeting.[118] The sanctions regime imposed against Iran is usually regarded as successful, at least to the extent that it achieved the goal of dragging Iran to the table to negotiate its nuclear programme. Yet, contrary to popular belief, it has been suggested that, what effectively pushed Iran was the pairing of economic sanctions with a credible and powerful threat of military retaliation.[119]

2.3.3 Step 8: Consider political willingness for and credibility of countermeasure

Finally, in the last step of decision-making, defenders must ensure enough political support and willingness for the countermeasure and confirm that the aggressors perceive retaliatory threats as credible. Since deterrence is a psychological game based on perceptions, defenders must build up their reputation by enhancing cross-governmental cooperation (*whole-of-government*), involving private stakeholders from the wider society (*whole-of-society*), and gaining international support against hybrid threats (*whole-of-alliance*), which is crucial to smaller powers, such as the Netherlands. This boosts the credibility of counter-hybrid postures.

Assess the credibility of the countermeasure in the eyes of the opponent

In classic deterrence theory, not only must the defender signal the ability and willingness to punish, but the aggressor must also be persuaded that the defender will do what it threatens, should a specific redline or behavioural benchmark be overstepped. In brief, the threat of punishment must be credible. However, credibility is not purely associated with the balance of forces on the field, but with the defender's actual and perceived strength. Whether an aggressor believes that a defender will deliver on its promises is mostly a matter of weighing and balancing the political interests underlying the respective conducts and how solid a deterrer's posture is from an organisational perspective.[120] The following key elements are characteristic of a credible response: (i) the actual and perceived strength of the military and non-military capabilities; (ii) the actual and perceived resolve to fulfil deterrent threats; (iii) the perceived intensity of the political commitment underlying deterrent threats; and (iv) the degree of national interests involved.[121] Whole of government, whole of society, and whole of system approaches boost the deterrer's credibility.

Assess the political willingness to adopt the countermeasure

Designing and implementing cross-domain responses against hybrid threats requires robust political support due to the issues in attribution, proportionality, and escalation management, as well as the risk of triggering second- and third-order effects that could undermine the

[118] Emma Ashford, 'Not-So-Smart Sanctions: The Failure of Western Restrictions Against Russia', *Foreign Affairs* 95, no. 1 (2016): 114–23.

[119] The Week, 'Do Economic Sanctions Actually Work?', *The Week UK* (blog), 23 February 2022.

[120] Vytautas Keršanskas, 'Deterrence: Proposing a More Strategic Approach To Countering Hybrid Threats' (Hybrid CoE, 9 March 2020), 22.

[121] Michael Mazarr et al., *What Deters and Why: Exploring Requirements for Effective Deterrence of Interstate Aggression* (RAND Corporation, 2018), 29.

credibility and legitimacy of the defender. The political commitment to fulfil deterrence threats must be robust and be perceived accordingly. The implementation of countermeasures should, therefore, be supported by broad political support at the domestic level. As better described below, a clear example of such commitments can be drawn from the adoption of a 'total defence' approach to hybrid threats by small European countries such as Estonia and Finland.[122] Moreover, especially for SMPs, assessing and ensuring political support on the international level is of paramount importance. States should foster political support and willingness to adopt countermeasures through international organisations, such as the EU, NATO, and the UN. In particular, states should seek the support of key allies to ensure that potential countermeasures are carried out more broadly.

Synchronise and coordinate domestic efforts: *whole-of-government* and *whole-of-society*

Policymakers must prioritise a whole-of-society approach to gain a competitive advantage over aggressors.

Concepts for a wider defence base to support military and nonmilitary responses, as well as coherent and transparent coordination across government branches and with private stakeholders, are crucial. First and foremost, policymakers must adopt a *whole-of-government* approach to synchronise military and civil efforts. However, coordination means that civil and military efforts shall remain separated to avoid escalation. In this regard, defence forces should not respond directly but merely provide governments with the appropriate means to deter, attribute, and respond in grey zones.[123] At the outset, efforts by defence forces will mostly focus on undertaking strategic intelligence operations to gather technical data across the political, military, economic, social, and information contexts, as well as disseminating insights across all governmental branches so as to favour detection and attribution.[124] Defence forces can also provide valuable options to enforce non-kinetic threats by using tools such as electronic warfare, cyber, intelligence, and reconnaissance. In the context of the EU, Finland's posture of total defence constitutes one of the most comprehensive *whole-of-government* approaches implemented to date. Finland has established a Security Committee, a permanent body that comprises 20 members and four experts from different branches of the government, as well as representatives of other official bodies and critical actors from the private sector. The Committee is tasked with improving cross-government and cross-societal collaboration to enhance comprehensive security and protect the vital interests of the state, under the perspective of both punishment and resilience.[125]

Given the prominent role of non-state actors in the hybrid environment, there is a need to move beyond classic like-minded groups of states and consider the role and contribution that civil society and private actors can make in countering hybrid threats. Policymakers must prioritise a *whole-of-society* approach to gain a competitive advantage over aggressors.[126] Companies operating in strategic sectors, such as telecommunications, energy, infrastructure, and military, are routinely targeted by hybrid activities, from malicious cyber operations to aggressive investments and disinformation. Consequently, companies inevitably become key

[122] Piotr Szymański, 'New Ideas for Total Defence. Comprehensive Security in Finland and Estonia' (Warszawa: Ośrodek Studiów Wschodnich im. Marka Karpia, 2020).

[123] Sean Monaghan, 'Countering Hybrid Warfare: So What for the Future Joint Force?', *PRISM* 8, no. 2 (October 2019): 83–98.

[124] Patrick J. Cullen and Erik Reichborn-Kjennerud, 'Understanding Hybrid Warfare' (Multinational Capability Development Campaign, January 2017), 4.

[125] Piotr Szymański, 'New Ideas for Total Defence. Comprehensive Security in Finland and Estonia', OSW Report (Warszawa: Ośrodek Studiów Wschodnich im. Marka Karpia, 2020).

[126] Jarno Limnell, 'Countering Hybrid Threats: Role of Private Sector Increasingly Important – Shared Responsibility Needed' (Hybrid CoE, 28 March 2018).

enablers of grey zone operations.[127] However, more importantly, the private sector is where the enforcement of countermeasures, such as sanctions, takes place. Hence, the effectiveness of counter-hybrid responses is also dependent upon the coordination between governments and private stakeholders.

Enhancing public-private partnerships allow for a better protection of critical interests and represents a powerful commitment to counter-hybrid threats.[128] Private companies can contribute to crafting strategies focused on resilience (*deterrence by denial*), as well as providing effective tools and inputs to respond actively and impose costs (*deterrence by punishment* and *entanglement*).[129] First, given their exposure to a large volume of real-time data, private companies are crucial to effective and comprehensive intelligence operations.[130] Second, by detecting, gathering, and sharing information, key private actors may help governments in the difficult task of attributing coercive and malicious conduct.[131] Third, given current entanglements and interconnectedness, big companies in strategic sectors have already started acting independently from their respective governments in countering aggressive operations.[132] Lastly, private stakeholders can actively participate in norm entrepreneurship[133] supporting non-profit organisations,[134] participating in multistakeholder initiatives,[135] and autonomously identifying industry best practices and standards of good behaviour.[136] A clear example of this approach can be seen in the latest Dutch cyber strategy, which devotes an entire pillar to developing an effective cooperation mechanism between public and private entities.[137] Furthermore, current discussions at the domestic, EU, and NATO levels are increasingly taking into account the crucial role that key private stakeholders play, and new legal frameworks are currently being designed and adopted. For instance, to respond to the regulatory vacuum that used to blur the activity of social media platforms[138], the EU is set

[127] John Schaus et al., ‘What Works: Countering Gray Zone Coercion’ (Centre for Strategic & International Studies, July 2018), 7.

[128] Limnell, ‘Countering Hybrid Threats: Role of Private Sector Increasingly Important. Shared Responsibility Needed’.

[129] Eugenio Lilli, ‘Redefining Deterrence in Cyberspace: Private Sector Contribution to National Strategies of Cyber Deterrence’, *Contemporary Security Policy* 42, no. 2 (3 April 2021): 163–88.

[130] David Artingstall and Nick Maxwell, ‘The Role of Financial Information-Sharing Partnerships in the Disruption of Crime’ (Royal United Services Institute, October 2017).

[131] Lilli, ‘Redefining Deterrence in Cyberspace’.

[132] See, for instance, Operation Aurora: ‘Operation Aurora - an Overview | ScienceDirect Topics’, ScienceDirect, accessed 10 June 2022. Operation Aurora was a cyber-enabled industrial espionage operation carried out by Chinese APTs targeting organizations, such as Adobe Systems, Juniper Networks, Rackspace, Yahoo, Symantec, Northrop Grumman, Morgan Stanley, and Dow Chemical, with the aim to gain access to and potentially modify source code repositories at these high tech, security and defense contractor companies. In response to the attack, Google decided to halt the provision of its services in China.

[133] Lilli, ‘Redefining Deterrence in Cyberspace‘, 177.

[134] Microsoft and Facebook are major sponsors of the Cyber Peace Institute, a non-governmental organization (NGO) which assists humanitarian NGOs to manage their cybersecurity: https://cyberpeaceinstitute.org/who-we-are/.

[135] USAID, ‘Multi-Stakeholder Initiatives with the Private Sector: Key Considerations and Decision-Making Framework’(2021). See, for instance, the Paris Call for Trust and Security in Cyberspace or the GAVI and Vaccine Alliance.

[136] See, for instance, Finance for Tomorrow, brings together asset managers and holders representing more than €4.3 trillion in the world’s first coalition of commitment to promote a just transition to low-carbon economies: https://financefortomorrow.com/. See also the Cyber security Tech Accord, a coalition of some of the most powerful tech companies aimed at promoting cyber-norms of responsible behaviour: https://cybertechaccord.org/.

[137] Ministerie van Justitie en Veiligheid, ‘Cabinet Presents New Cybersecurity Strategy - News Item - Government.Nl’, nieuwsbericht (Ministerie van Algemene Zaken, 10 October 2022).

[138] See Karen Hao, ‘How Facebook and Google Fund Global Misinformation’, *MIT Technology Review*, accessed 10 June 2022.

to adopt the Digital Service Act, which aims to protect the fundamental rights of users from online manipulative content and the exchange of illegal services.[139]

As previously anticipated, the insufficient involvement of private stakeholders also hinders the enforcement of responses. Private companies are incentivised to dodge countermeasures without their governments' proper engagement to maximise their profits.[140] Yet, one of the biggest challenges to adopting a comprehensive multistakeholder approach is understanding how to apply it. The relationship between the government and the private sector could be framed as either a principal-agent relationship or as independent and mutual cooperation. The first notion considers the private sector as 'a government capability in reserve [...]' while the second considers private stakeholders as 'fully capable actor(s) in [their] own right'.[141] Thus framed, governments may decide to involve private stakeholders through either: (i) coercion (through law and regulations), (ii) co-option (through positive inducement), and (iii) conviction (*i.e.*, the ability to convince non-state actors to cooperate voluntarily). In the latter regard, liberal democracies must strive to convince relevant non-state actors to voluntarily cooperate with the crafting of counter-hybrid strategies.

Synchronise and coordinate international efforts

Through a *whole-of-system* approach, defenders must act in conjunction with international allies.

Besides national engagement, there is an obvious need to involve international stakeholders in enacting the countermeasures, especially for smaller states like the Netherlands. Through a *whole-of-system* approach, defenders must act in conjunction with international allies. International cooperation must be promoted through international organisations, such as the EU, NATO, and the UN. Efforts are already underway as the EU is developing a framework for a coordinated EU response to hybrid campaigns, while NATO is developing a set of comprehensive preventive and response options to hybrid threats.[142] In addition to international organisations, multinational companies, such as large Internet platforms or service providers, and civil society organizations must also be involved. This approach aims to identify ways in which allies and partners can cooperate to achieve shared strategic objectives, despite the inevitable heterogeneity among the actors on key aspects, such as the setting of broadly shared red bands of unacceptable behaviour, or different capabilities. Interestingly, the need to develop this approach was initially promoted by international non-state actors dealing with cybersecurity and Internet governance, such as the Internet Corporation for Assigned Names and Numbers (ICANN) and the Internet Engineering Task Force (IETF).[143] Whenever possible, defenders must boost international dialogue through diplomacy and norm development.

[139] European Commission, 'The Digital Services Act Package | Shaping Europe's Digital Future', European Commission, accessed 17 November 2022.

[140] Francesco Giumelli and Michal Onderco, 'States, Firms, and Security: How Private Actors Implement Sanctions, Lessons Learned from the Netherlands', *European Journal of International Security* 6, no. 2 (May 2021): 190–209.

[141] Alexander Klimburg, 'The Whole of Nation in Cyberpower', *Georgetown Journal of International Affairs*, 2011, 173.

[142] European Council, 'Council Conclusions on a Framework for a Coordinated EU Response to Hybrid Campaigns', European Council, 21 June 2022; Michael Ruhle and Clare Roberts, 'Enlarging NATO's Toolbox to Counter Hybrid Threats', NATO Review, 19 March 2021.

[143] Louk Faesen et al., 'The Promises and Perils of a Minimum Cyber Deterrence Posture' (The Hague Center for Strategic Studies, 2022), 58.

2.4 The Execution Stage

In the Execution Stage, the chosen action should be appropriately and efficiently executed.

2.4.1 Step 9: Engage in appropriate and efficient execution

Retaliatory threats and countermeasures must be executed appropriately. This requires defenders to manage time effectively, consolidate public support, signal consistently through meaningful strategic communication, and monitor whether responses alter the opponent's cost-benefit calculus. Smaller powers, such as the Netherlands, should consider executing counter-hybrid responses in conjunction with other like-minded partners.

Implement a timely warning response with reference to vital interests and threats of punishment

Hybrid threats are traditionally challenging to anticipate, let alone to deter. In either case, it is crucial to parse and execute responses promptly. In the hybrid context, the notion of 'timely' action does not necessarily entail that responses should be 'immediate'. In some circumstances, the most appropriate timing may coincide with the moment in which efforts have been synchronised with partners across different levels. Conversely, hybrid operations which traditionally occur in a continuum, such as disinformation and cyber-attacks, are best countered through a permanently integrated effort. It has also been suggested that a successful deterrence posture may benefit from strategic delays in responding to hybrid threats, to the extent that this allows taking advantage of ambiguity and synchronising efforts with like-minded partners. The cross-domain and asymmetrical nature of hybrid threats and counter-hybrid responses also entails that different tools of powers and responses may be deployed simultaneously. Hence, the concept of a timely response is dependent on the measure a defender seeks to implement to counter grey-zone aggression.

Monitor domestic and international support

Defenders must ensure that responses keep receiving public support, both domestically and at the international level. Public support, at least from like-minded states, is strictly correlated to the proportionality and credibility of retaliatory threats. For example, the use of violent means – such as military or cyber-attacks having kinetic effects, against harmful yet non-violent conducts, such as theft, espionage, infiltration, or election meddling, is likely to be perceived by many as disproportionate.[144] Furthermore, defenders should always consider that different actors, either states or non-state actors, all have their individual perceptions as to what constitutes a proportional response. Hence, in the Execution Stage, defenders must constantly monitor public support for the countermeasure implemented. Using violence against non-violent hostilities is likely to be seen as disproportionate by many.

Keep strategic goals at the centre

Defined strategic goals should be the leading factors when responding across domains. Consequently, defenders should keep political and strategic objectives – rather than the

[144] As Richard Andres notes, 'while the United States could threaten to retaliate against cyberattacks asymmetrically through economic sanctions or military threats, there is a significant chance that such actions would appear escalatory, disproportionate, or otherwise inappropriate to the American public or the international community.'' See Richard Andres, 'Cyber Gray Space Deterrence', *PRISM | National Defense University* 7, no. 2 (2017).

tactical and operational ones – front and centre. Narratives affect the adversary's perception of the defender's resolve and reduce or enlarge the space for misunderstanding. For instance, if a defender assumes an injured innocent posture when suffering an attack, adopting overt and even covert responses could be a setback. On the contrary, if a state's narrative is based on 'resolute defence', then disproportionate retaliation plays an important role early on. The centrality of narrative avoids the bottom-up problem of placing the tactical before the political and helps solve issues related to path dependency. Path dependency is particularly evident in the cyber domain, characterised by a natural trend favouring technical operators and a 'bottom-up culture of putting technical feasibility before political desirability.'[145] Prioritising strategic goals over tactical and operational ones also helps establish red bands and a more comprehensive assessment of the equities that, in contrast to tactical assessments, may lead to a different response because of the broader strategic or geopolitical environment.[146]

Execute synchronised and coordinated government wide, multilevel StratCom

In the hybrid environment, it is crucial to build and visualise the relevant information environment, which is a conceptual model that consists of a *physical* (who are the relevant actors involved), a *cognitive* (how different actors process information), and an *informational* (through what means is the information delivered and received) dimension.[147] StratCom must be crafted and adapted based on the specific actor to deter (it could be a government, a political leader, a non-state actor such as international organisations or government-organised non-governmental organisations, etc.), the type of threat (economic coercion, disinformation, electoral influence, etc.), as well as the domain in which it operates (economic, cyber, diplomatic, military, etc.).[148]

Defined strategic goals should be the leading factors when responding across domains.

Strategic communication must be synchronised across all branches of government, rather than inconsistently depending on the military, and control over the narrative and associated messaging '[...] must be factored in from the start'[149] and understood as an 'organisational responsibility'.[150] StratCom must not be limited to press offices or the publication of official statements, doctrines, and strategies: governments should invest in disseminating strategic messages to boost a coherent and credible posture in line with the guiding principles and values pursued. As an overarching tool that informs the overall strategy, effective StratCom must be targeted towards one's population and key stakeholders (such as companies, organisations, etc.) to raise societal awareness and enhance resilience.[151] It must target like-minded partners through diplomatic, legal, military, and economic cooperation to gain strategic support and boost unity of intent at the international level. Finally, it is crucial that the message effectively targets the opponent engaging in hybrid operations.[152]

[145] Alexander Klimburg, *The Darkening Web: The War for Cyberspace* (Penguin Press, 2017). 149-50.

[146] Klimburg, *The Darkening Web*, 2017, 200.

[147] See US Army, 'Joint Publication 3-13. Information Operations' accessed June 1, 2022.

[148] Una Aleksandra et al., 'Hybrid Threats: A Strategic Communications Perspectives' (NATO Strategic Communications Centre of Excellence, 2019), 9.

[149] James Pamment et al., 'Hybrid Threats: Confucius Institutes' (NATO Strategic Communications Centre of Excellence, 6 June 2019).

[150] Elina Lange-Ionatamisvili et al., 'Georgia's Information Environment through the Lens of Russia's Influence' (NATO Strategic Communications Centre of Excellence, 2021), 12.

[151] In 2009, the Swedish government established the Civil Contingencies Agency (MSB) as a combination of the Rescue Services Agency, the Emergency Management Agency and the National Board of Psychological Defence. After the Russian hybrid campaign against Ukraine in 2014-2015, the MSB has routinely been tasked with developing communication campaigns to raise awareness with regard to foreign attempts to influence elections. See 'MSB – The Swedish Civil Contingencies Agency', accessed 2 June 2022.

[152] Juan Pablo Villar García et al., 'Strategic Communications as a Key Factor in Countering Hybrid Threats.' (European Parliament, 2021).

At the international level, defenders must promote proactive narratives based on common guiding principles and strategic objectives to boost legitimacy and political support.[153] An example of an international StratCom effort is the EU East StratCom Task Force, which attempts to forecast, address, and respond to Russia's ongoing disinformation campaigns affecting member states from Eastern Europe.

2.5 The Evaluation Stage

In the Evaluation Stage, the entire process and the execution of the hybrid response option must be evaluated.

2.5.1 Step 10: Assess effectiveness of countermeasure

It is crucial for the success of deterrence to constantly monitor whether a chosen strategy is effectively reaching the desired objective.

It is crucial for the success of deterrence to constantly monitor whether a chosen strategy is effectively reaching the desired objective, namely whether it (i) effectively influences the adversary's behaviour by altering its cost-benefit calculus, (ii) it avoids vertical escalation and reduces the breadth of horizontal escalation, (iii) limits second- and third-order effects, and (iv) to maintain broad support at the domestic and international levels. Depending on their nature, scope, and magnitude, it may take more or less time to assess the countermeasures'' effectiveness (or ineffectiveness). By any means, whenever any of the previous objectives are not concretely met, deterrence strategies are likely to be either ineffective (as it fails to influence the adversary's behaviour), inefficient (as it achieves their objective but at a high cost for the defender), or even detrimental (as it triggers escalation or backfires).

Evaluate attainment of cost-imposition objective

Relevant strategies enacted against hybrid influence and coercion in recent years can be analysed retrospectively to assess whether specific responses succeeded in deterring hybrid actors. For instance, in response to Chinese economic espionage, the U.S. opted for indictments at the tactical level and the threat of sanctions at the strategic level while exerting high-level political engagement between Obama and Xi. Contrary to what happened in the economic domain, the U.S. strategy eventually led to the signing of a bilateral agreement and, therefore, can be considered successful. While operating across different domains and at various levels, Washington consistently and uniformly signalled to Beijing that cyber-enabled IP theft was unacceptable and that the U.S. was willing to escalate the issue while at the same time offering incentives. Cumulatively, while still containing the risk of unintended second-order effects, the U.S. strategy favoured multiple avenues for reinforcement even when overt moves were employed. The initial responses created sufficient leverage for bilateral negotiations to mitigate escalation by establishing an agreement between the competitors.[154] While assessing and measuring espionage trends and impact is inevitably challenging, many agreed that there was a noticeable drop in Chinese economic espionage targeting the U.S. in the year following the agreement, albeit with disagreement regarding the underlying reasons for the decrease and explanations as to why and how it resurged from 2017 onwards.[155]

[153] European External Action Service, 'Questions and Answers about the East StratCom Task Force', accessed 2 June 2022.

[154] Louk Faesen et al., 'The Promises and Perils of a Minimum Cyber Deterrence Posture', 53.

[155] Louk Faesen et al., 'From Blurred Lines to Red Lines', 91.

Evaluate escalatory dynamics

Assessing escalatory dynamics is crucial at both the Decision-Making and Execution Stages. Defenders should strive to monitor the consequences of the measures deployed, as such consequences are likely to impact their long-term strategic goals. This is because countermeasures can easily set new precedents for escalatory responses in peacetime. In this regard, overt coercive countermeasures (including the leaking of covert measures) have the most considerable propensity for inadvertent effects.

Evaluate second- and third-order effects

States must constantly monitor whether the chosen response is likely to trigger or has already triggered second- and third-order effects. For instance, unlike conventional weapons, cyber operations can target more accurately with less physical collateral damage. However, the risk and extent of potential second- and third-order effects is undeniably vast in the hybrid domain. Indeed, cyber effects can occur outside the area of operation, in domains other than cyberspace, and can undermine the security of other (neutral, allied or civilian) actors that rely on the same system – NotPetya being an infamous example. Economic and financial sanctions, for instance, are likely to trigger significant second- and third-order effects. The decision by the Trump administration to impose severe unilateral countervailing duties, for an estimated annual trade value of 250 billion USD on Chinese goods in response to alleged 'unfair trade practices'[156] was taken in an attempt to counter the strategy of economic coercion, which had been putting U.S. companies in a condition of 'competitive disadvantage' and causing a significant trade deficit between the countries. Regardless of its broader political value, from the perspective of cost-benefit calculations, the decision by the U.S. to respond 'symmetrically' did not attain the desired objectives. First, while undoubtedly imposing some costs on China, massive trade sanctions were unable to effectively alter Chinese behaviour and ultimately missed their objective to revitalise the U.S. manufacturing industry and deter economic coercion.[157] A recent report highlighted that, while achieving progress on existing trade barriers in sectors such as agriculture and finance, the measures failed to effectively curb the majority of Chinese aggressive policies, specifically related to market access and non-market economies (NMEs), that the U.S. considered distortive. The imposition of massive retaliatory trade measures on the world's biggest economy inevitably had ripple effects in global markets.[158] The weakening of the Yuan raised China's borrowing costs, thus slowing down the world economy. Furthermore, the shift in global trade due to U.S. sanctions and correspondent Chinese retaliatory measures disrupted chains in several sectors. From a political perspective, U.S. decisions attracted significant criticism from its partners, including the EU, which sought to balance and counter the effects of U.S. measures.[159] From a normative perspective, the measures adopted by the U.S. eventually caused two significant consequences. First, China gained credibility by challenging U.S. measures before the WTO dispute settlement body and ultimately winning the case.[160] Second, it led to further escalatory consequences when the U.S. vented its frustration by blocking the appointment of new panellists at the WTO Dispute Settlement Body (DSB), thus dismantling one of the core features of

[156] Office of the United States Trade Representative, 'Investigation: Technology Transfer, Intellectual Property, and Innovation', United States Trade Representative, accessed 17 June 2022.

[157] Josh Zumbrun and Bob Davis, 'China Trade War Didn't Boost U.S. Manufacturing Might', *Wall Street Journal*, 25 October 2020, sec. Politics.

[158] Davin Chor and Bingjing Li, 'The Impact of the US-China Tariff War on China's Economy'.

[159] Jack Ewing, 'Europe Retaliates Against Trump Tariffs', *The New York Times*, 21 June 2018, sec. Business.

[160] See WTO, 'DS534: Tariff Measures on Certain Goods from China', WTO, accessed 13 December 2022. In particular, the panel found that the U.S. violated the MFN treatment, its schedules of concessions towards China and that the measures were not justified under GATT Art. XX(a) for protecting public morals.

the multilateral trade forum. In sum, responding symmetrically to Chinese economic warfare is proving ineffective under many circumstances. Not only did U.S. measures cause significant economic and financial losses worldwide, but – from a normative perspective – there is a risk that they could severely undermine established international norms of trade cooperation.[161]

Table 3 summarises the actions along each of the steps of the response framework.

Table 3: The actions required in each step of the response framework.

Stages	Steps	Actions
Preparation	**Step 1: Set red bands of unacceptable behaviour**	1. Parse the spectrum of adversarial hybrid operations based on their impact, marking which ones will prompt a response. 2. Set red bands of unacceptable behaviour 3. Communicate the red bands of unacceptable behaviour internally, with partners, and possibly with adversaries. 4. Encourage positive behaviour through reassurances, incentives, and norm setting.
	Step 2: Signal ability and will to punish	5. Signal ability and will to deliver on deterrence promises, possibly through the demonstration of capability and announcement of commitment.
	Step 3: Enhance ability to detect and attribute	6. Increase detection capability. 7. Strengthen ability to attribute within a politically meaningful timeframe. 8. Prepare to convincingly explain attribution to third parties.
Detection & Attribution	**Step 4: Detect hybrid attack**	9. Detect hybrid attack.
	Step 5: Consider attribution options	10. Decide whether to attribute. 11. Attribute in an effective manner.
Decision-making	**Step 6: Choose response options**	12. Parse the available countermeasures across the DIMEFIL spectrum according to their impact. 13. Identify possible targets across multiple domains, including counterforce, countervalue, and counter-political targets. 14. Assess the legality of the response options. 15. Assess the duration and the timeframe within which they come into effect. 16. Consider the proportionality of the countermeasure. 17. Identify entanglements and second- and third-order effects. 18. Conduct an escalation assessment.
	Step 7: Assess effectiveness of response on adversarial cost-imposition perception	19. Examine costs at the psychological level. 20. Examine costs at the political level. 21. Examine costs at the economic and operational level.
	Step 8: Consider political willingness for and credibility of countermeasure	22. Assess the credibility of the countermeasure in the eyes of the opponent. 23. Assess the political willingness to adopt the countermeasure. 24. Synchronise and coordinate domestic efforts: *whole-of-government* and *whole-of-society.* 25. Synchronise and coordinate international efforts.
Execution	**Step 9: Execute response option and implement countermeasures**	26. Implement a timely warning response with reference to vital interests and threat of punishment. 27. Monitor domestic and international support. 28. Keep strategic goals at the centre. 29. Execute synchronised and coordinated government-wide, multilevel StratCom.
Evaluation	**Step 10: Assess effectiveness of countermeasure**	30. Evaluate attainment of cost-imposition objective. 31. Evaluate escalatory dynamics. 32. Evaluate second- and third-order effects.

[161] Aaron Seals, 'Dismantling the WTO: The United States' Battle Against World Trade,' University of Miami Business Law Review (2019).

3. The Way Forward

Over the past decade, policy efforts to counter hybrid threats within Western SMPs have had considerable momentum. Counter-hybrid units were created, budgets allocated, strategies drafted, national and international consultation and coordination mechanisms established, a growing body of legal frameworks adopted, and an assortment of policy measures implemented. All these efforts contributed to the goal to address hybrid threats that were intended to circumvent detection, existing rules and regulation, and response thresholds to minimise the basis for decisive responses. The counter-hybrid toolbox of most Western SMPs now includes preventive resilience as well as proactive response measures including the punishment of violations with an eye to deterring their future occurrence.

Now is the time to take the next step in the counter-hybrid policy realm.

The policy guidelines offered in this report will help inform the execution of the deterrence component of SMP's counter-hybrid postures. The guidelines offer practical insights on how to craft and execute proportional, legitimate, and effective countermeasures to deter actors operating in the grey zone, while simultaneously managing escalation and anticipating potential second- and third-order effects. The design and execution of such countermeasures need to be synchronised between different branches of government, require close cooperation with international partners, and will sometimes necessitate the involvement of private sector actors. Now is the time to take the next step in the counter-hybrid policy realm. To that purpose, we offer three recommendations to policymakers from SMPs to take this forward:

1. Convene an international symposium with representatives from SMPs to discuss how these policy guidelines can guide the further development of counter-hybrid efforts at the national and international level. The Counter Hybrid Threat Centre of Excellence in Helsinki is well positioned to spearhead this effort.

2. Adopt and adapt these policy guidelines to the specific institutional and policy planning cycle contexts. This of course lies within the national competencies of individual SMPs.

3. Deploy the policy guidelines within the context of a real-world counter-hybrid campaign. Such a campaign can be executed by individual SMPs or, as suggested in this report, by SMPs closely working together with partners in bilateral and multilateral partnerships. It is recommended that The Netherlands in collaboration with one or multiple selected partner countries takes the lead in this endeavour. Such campaigns can first be practiced in simulations and serious gaming.

Bibliography

Acton, James M. 'Cyber Warfare & Inadvertent Escalation.' *Daedalus* 149, no. 2 (2020): 133–49. https://www.jstor.org/stable/48591317.

AJIL. 'United States Continues to Block New Appellate Body Members for the World Trade Organization, Risking the Collapse of the Appellate Process.' *American Journal of International Law* 113, no. 4 (October 2019): 822–31. https://doi.org/10.1017/ajil.2019.59.

Aleksandra, Una, Berzina Cerenkova, James Pamment, Vladimir Sazonov, Francesca Granelli, Sean Aday, Maris Andzans, et al. 'Hybrid Threats: A Strategic Communications Perspectives.' NATO Strategic Communications Centre of Excellence, 2019. https://stratcomcoe.org/publications/hybrid-threats-a-strategic-communications-perspective/79.

Altman, Daniel W. 'Redlines and Faits Accomplis in Interstate Coercion and Crisis.' Thesis, Massachusetts Institute of Technology, 2015. https://dspace.mit.edu/handle/1721.1/99775.

Andres, Richard. 'Cyber Gray Space Deterrence.' *PRISM | National Defense University* 7, no. 2 (2017). http://cco.ndu.edu/News/Article/1401927/cyber-gray-space-deterrence/.

Artingstall, David. 'The Role of Financial Information-Sharing Partnerships in the Disruption of Crime.' Accessed June 10, 2022. https://rusi.org/explore-our-research/publications/occasional-papers/role-financial-information-sharing-partnerships-disruption-crime.

Ashford, Emma. 'Not-so-Smart Sanctions: The Failure of Western Restrictions Against Russia.' *Foreign Affairs* 95 (2016): 114–23. https://www.jstor.org/stable/43946631.

Bajarūnas, Eitvydas. 'Addressing Hybrid Threats: Priorities for the EU in 2020 and Beyond.' *European View* 19, no. 1 (April 1, 2020): 62–70. https://doi.org/10.1177/1781685820912041.

Bar, Shmuel. 'God, Nations, and Deterrence: The Impact of Religion on Deterrence.' *Comparative Strategy* 30, no. 5 (December 14, 2011): 428–52. https://doi.org/10.1080/01495933.2011.624808.

BBC. 'UK Launched Cyber-Attack on Islamic State.' *BBC News*, April 12, 2018, sec. Technology. https://www.bbc.com/news/technology-43738953.

Benner, Katie, and Sharon LaFraniere. 'Justice Dept. Moves to Drop Charges Against Russian Firms Filed by Mueller.' *The New York Times*, March 16, 2020, sec. U.S. https://www.nytimes.com/2020/03/16/us/politics/concord-case-russian-interference.html.

Berejikian, Jeffrey D. 'A Cognitive Theory of Deterrence.' *Journal of Peace Research* 39, no. 2 (2002): 165–83. https://www.jstor.org/stable/1555297.

Bishai, Linda. 'The Many Faces of Power.' Edited by Felix Berenskoetter and Michael J. Williams. *International Studies Review* 10, no. 4 (2008): 798–800. https://www.jstor.org/stable/25482027.

Brantly, Aaron. 'Back to Reality: Cross Domain Deterrence and Cyberspace.' SSRN Scholarly Paper. Rochester, NY, September 1, 2018. https://doi.org/10.2139/ssrn.3256666.

Brown, Michael E. 'Deterrence Failures and Deterrence Strategies: Or, Did You Ever Have One of Those Days When No Deterrent Seemed Adequate?' RAND Corporation, 1977. https://www.rand.org/pubs/papers/P5842.html.

Cassidy, John. 'Iran Nuke Deal: Do Economic Sanctions Work After All?' *The New Yorker*, November 25, 2013. http://www.newyorker.com/news/john-cassidy/iran-nuke-deal-do-economic-sanctions-work-after-all.

Cesarini, Paolo. 'Regulating Big Tech to Counter Online Disinformation: Avoiding Pitfalls while Moving Forward.' *MediaLaws* 1 (2021). https://www.medialaws.eu/rivista/regulating-big-tech-to-counter-online-disinformation-avoiding-pitfalls-while-moving-forward/.

Chappell, Bill, and Carrie Johnson. 'U.S. Charges 7 Russian Intelligence Officers With Hacking 40 Sports And Doping Groups.' *NPR*, October 4, 2018, sec. Europe. https://www.npr.org/2018/10/04/654306774/russian-cyber-unit-accused-of-attacking-opcw-chemical-weapons-watchdog.

Chor, Davin, and Bingjing Li. 'The Impact of the US-China Tariff War on China's Economy: New Evidence from Night-Time Lights.' *VoxEU.Org* (blog), November 25, 2021. https://voxeu.org/article/us-china-tariff-war-and-china-s-economy-evidence-night-lights.

———. 'The Impact of the US-China Tariff War on China's Economy: New Evidence from Night-Time Lights.' *VoxEU.Org* (blog), November 25, 2021. https://voxeu.org/article/us-china-tariff-war-and-china-s-economy-evidence-night-lights.

Courtney, Chris Kremidas. 'The Vital Role of Public-Private Partnerships in Countering Hybrid Threats.' *Friends of Europe* (blog). Accessed June 10, 2022. https://www.friendsofeurope.org/insights/the-vital-role-of-public-private-partnerships-in-countering-hybrid-threats/.

Creswell, Michael H. 'Wasted Words? The Limitations of U.S. Strategic Communication and Public Diplomacy.' *Studies in Conflict & Terrorism* 42, no. 5 (May 4, 2019): 464–92. https://doi.org/10.1080/1057610X.2017.1392097.

Cullen, Patrick J., and Erik Reichborn-Kjennerud. 'Understanding Hybrid Warfare.' Multinational Capability Development Campaign, n.d. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/647776/dar_mcdc_hybrid_warfare.pdf.

Daniel, Michael. 'Closing the Gap: Expanding Cyber Deterrence.' *Cyberstability Paper Series*, 2021, 12.

Davis, Josh Zumbrun and Bob. 'China Trade War Didn't Boost U.S. Manufacturing Might.' *Wall Street Journal*, October 25, 2020, sec. Politics. https://www.wsj.com/articles/china-trade-war-didnt-boost-u-s-manufacturing-might-11603618203.

Davis, Paul K., Angela O'Mahony, Christian Curriden, and Jonathan Lamb. 'Influencing Adversary States: Quelling Perfect Storms.' RAND Corporation, February 16, 2021. https://www.rand.org/pubs/research_reports/RRA161-1.html.

DePetris, Daniel R. 'When Deterrence Failed: Why Saddam Hussein Invaded Kuwait.' Text. *The National Interest* (blog). The Center for the National Interest, November 27, 2018. https://nationalinterest.org/blog/skeptics/when-deterrence-failed-why-saddam-hussein-invaded-kuwait-37237.

Deutsche Welle (www.dw.com). 'US Expels Russian Diplomats and Issues Sanctions over SolarWinds Hacking Attack | DW | 15.04.2021.' DW.COM. Accessed April 29, 2022. https://www.dw.com/en/us-expels-russian-diplomats-and-issues-sanctions-over-solarwinds-hacking-attack/a-57215141.

Dilanian, Ken, and Courtney Kube. 'Biden given Options for Unprecedented Cyberattacks against Russia.' *NBC News*. Accessed May 16, 2022. https://www.nbcnews.com/politics/national-security/biden-presented-options-massive-cyberattacks-russia-rcna17558.

Federation Of American Scientists. 'DoD 'Clarifies' Doctrine on Psychological Operations.' Accessed June 22, 2022. https://fas.org/blogs/secrecy/2010/01/psyop/.

Ekman, Colonel Kenneth P. 'Applying Cost Imposition Strategies Against China,' 2015, 34.

———. 'Winning the Peace Through Cost Imposition.' *Foreign Policy*, n.d., 64.

Ellehuus, Rachel. 'Strange Birds in the Archipelago: Finland's Legislation on Foreign Real Estate Investment.' *Kremlin Plabook Spotlight* (blog). Accessed June 14, 2022. https://www.csis.org/blogs/kremlin-playbook-spotlight/strange-birds-archipelago-finlands-legislation-foreign-real-estate.

European Commission - European Commission. 'EU Foreign Investment Screening Mechanism.' Text. Accessed June 22, 2022. https://ec.europa.eu/commission/presscorner/detail/en/ip_20_1867.

'EU Initiates WTO Dispute Complaint Regarding Chinese Restrictions on Trade with Lithuania.' Accessed June 10, 2022. https://www.wto.org/english/news_e/news22_e/ds610rfc_31jan22_e.htm.

European Commission. 'Answer for Question E-002880/19,' 2020. https://www.europarl.europa.eu/doceo/document/E-9-2019-002880-ASW_EN.html.

———. 'Commission Proposal for an Anti-Coercion Instrument,' 2021. https://trade.ec.europa.eu/doclib/docs/2021/december/tradoc_159958.pdf.

———. 'Commission Proposal for an Anti-Coercion Instrument,' 2021. https://trade.ec.europa.eu/doclib/docs/2021/december/tradoc_159958.pdf.

———. 'Communication: The European Economic and Financial System: Fostering Openness, Strength and Resilience.' Accessed May 16, 2022. https://ec.europa.eu/info/publications/210119-economic-financial-system-communication_en.

———. 'EU Strengthens Protection against Economic Coercion.' Text. European Commission - European Commission. Accessed May 16, 2022. https://ec.europa.eu/commission/presscorner/detail/en/ip_21_6642.

European External Action Service. 'About.' EU vs Disinfo. Accessed June 2, 2022. https://euvsdisinfo.eu/about/.

———. 'Questions and Answers about the East StratCom Task Force.' Accessed June 2, 2022. https://www.eeas.europa.eu/eeas/questions-and-answers-about-east-stratcom-task-force_en.

———. 'Strategic Communications | EEAS Website.' Accessed June 13, 2022. https://www.eeas.europa.eu/taxonomy/term/400164_en.

European Parliament. Directorate General for Parliamentary Research Services. *Strategic Communications as a Key Factor in Countering Hybrid Threats.* LU: Publications Office, 2021. https://data.europa.eu/doi/10.2861/14410.

Ewing, Jack. 'Europe Retaliates Against Trump Tariffs.' *The New York Times*, June 21, 2018, sec. Business. https://www.nytimes.com/2018/06/21/business/economy/europe-tariffs-trump-trade.html.

Eyes on Europe. 'How the EU should respond to the new US sanctions against Russia?' *Eyes on Europe* (blog), August 23, 2017. https://www.eyes-on-europe.eu/how-eu-us-sanctions-against-russia/.

Fabry, Elvire, and Erik Tate. 'Saving the WTO Appellate Body or Returning to the Wild West of Trade?' Jaccques Delors Institute. Accessed June 17, 2022. https://institutdelors.eu/en/publications/sauver-lorgane-dappel-de-lomc-ou-revenir-au-far-west-commercial/.

Faesen, Louk, Alexander Klimburg, and Michel Rademaker. 'Cyber Arms Watch.' The Hague Center for Strategic Studies. Accessed June 21, 2022. https://hcss.nl/cyber-arms-watch/.

Faesen, Louk, Tim Sweijs, Alexander Klimburg, Conor MacNamara, and Michael Mazarr. 'From Blurredlines to Redlines.' The Hague Center for Strategic Studies, 2020. https://hcss.nl/news/new-report-from-blurred-lines-to-red-lines-countermeasures-and-norms-in-hybrid-conflict/.

Faesen, Louk, Tim Sweijs, Alexander Klimburg, and Giulia Tesauro. 'The Promises and Perils of a Minimum Cyber Deterrence Posture.' The Hague Center for Strategic Studies, 2022. https://hcss.nl/wp-content/uploads/2022/04/Cyber-Deterrence-Final.pdf.

Fallon, Hon Sir Michael. 'Defence Secretary Sir Michael Fallon Hails Importance of UK's Defence Network.' Accessed May 16, 2022. https://www.gov.uk/government/news/defence-secretary-sir-michael-fallon-hails-importance-of-uks-defence-network.

'Finance for Tomorrow - The Sustainable Future Begins in Paris.' Accessed June 10, 2022. https://financefortomorrow.com/.

Fischerkeller, Michael P., and Richard J. Harknett. 'Persistent Engagement and Cost Imposition: Distinguishing Between Cause and Effect.' Lawfare, February 6, 2020. https://www.lawfareblog.com/persistent-engagement-and-cost-imposition-distinguishing-between-cause-and-effect.

Frantzen, Henning-A. 'Hybrid Deterrence.' Report. *8*, 2020. https://fhs.brage.unit.no/fhs-xmlui/bitstream/handle/11250/2636837/IFS%20Insight%201_2020_oppdatert.pdf?sequence=5&isAllowed=y.

———. 'Hybrid Deterrence.' Report. *8*, 2020. https://fhs.brage.unit.no/fhs-xmlui/handle/11250/2636837.

Freedman, Lawrence. 'Introduction — The Evolution of Deterrence Strategy and Research.' In *NL ARMS Netherlands Annual Review of Military Studies 2020*, edited by Frans Osinga and Tim Sweijs, 1–10. NL ARMS. The Hague: T.M.C. Asser Press, 2021. https://doi.org/10.1007/978-94-6265-419-8_1.

Garamone, Jim. 'Concept of Integrated Deterrence Will Be Key to National Defense Strategy, DOD Official Sa.' U.S. Department of Defense. Accessed May 9, 2022. https://www.defense.gov/News/News-Stories/Article/Article/2866963/concept-of-integrated-deterrence-will-be-key-to-national-defense-strategy-dod-o/.

García, Juan Pablo Villar, Carlota Tarín Quirós, Julio Blázquez Soria, Carlos Galán Pascual, and Carlos Galán Cordero. 'Strategic Communications as a Key Factor in Countering Hybrid Threats.' LU: European Parliament, 2021. https://data.europa.eu/doi/10.2861/14410.

Gartzke, Eric, and Jon R. Lindsay. *Cross-Domain Deterrence: Strategy in an Era of Complexity*. New York: Oxford University Press, 2019. https://doi.org/10.1093/oso/9780190908645.001.0001.

Gill, Monika, Ben Heap, and Pia Hansen. 'Strategic Communications Hybrid Threats Toolkit.' NATO Strategic Communications Centre of Excellence. Accessed June 2, 2022. https://stratcomcoe.org/publications/strategic-communications-hybrid-threats-toolkit/213.

Giumelli, Francesco, and Michal Onderco. 'States, Firms, and Security: How Private Actors Implement Sanctions, Lessons Learned from the Netherlands.' *European Journal of International Security* 6, no. 2 (May 2021): 190–209. https://doi.org/10.1017/eis.2020.21.

Griswold, Daniel. 'Four Decades of Failure: The U.S. Embargo against Cuba.' CATO Institute, 2005. https://www.cato.org/speeches/four-decades-failure-us-embargo-against-cuba.

Haass, Richard N. 'Economic Sanctions: Too Much of a Bad Thing.' *Brookings* (blog), November 30, 1AD. https://www.brookings.edu/research/economic-sanctions-too-much-of-a-bad-thing/.

Hackenbroich, Jonathan, and Pawel Zerka. 'Measured Response: How to Design a European Instrument against Economic Coercion.' European Council on Foreign Relations, June 23, 2021. https://ecfr.eu/publication/measured-response-how-to-design-a-european-instrument-against-economic-coercion/.

Hagan, Joe D. 'Diversionary Theory of War in Foreign Policy Analysis.' Oxford Research Encyclopedia of Politics, October 26, 2017. https://doi.org/10.1093/acrefore/9780190228637.013.412.

Hanania, Richard. 'Ineffective, Immoral, Politically Convenient: America's Overreliance on Economic Sanctions and What to Do about It.' *Cato Institute* (blog), February 18, 2020. https://www.cato.org/policy-analysis/ineffective-immoral-politically-convenient-americas-overreliance-economic-sanctions.

Hao, Karen. 'How Facebook and Google Fund Global Misinformation.' *MIT Technology Review*, 2021. https://www.technologyreview.com/2021/11/20/1039076/facebook-google-disinformation-clickbait/.

Haworth, Jessica. 'Russian Hacking Group APT28 'Conducting Brute-Force Attacks' against Organizations Worldwide.' The Daily Swig | Cybersecurity news and views, July 2, 2021. https://portswigger.net/daily-swig/russian-hacking-group-apt28-conducting-brute-force-attacks-against-organizations-worldwide.

Higgins, Andrew. 'Expelling Diplomats, a Furious Kremlin Escalates a Crisis.' *The New York Times*, March 29, 2018, sec. World. https://www.nytimes.com/2018/03/29/world/europe/russia-expels-diplomats.html.

Iasiello, Emilio. 'Is Cyber Deterrence an Illusory Course of Action?' *Journal of Strategic Security* 7, no. 1 (March 2014): 54–67. https://doi.org/10.5038/1944-0472.7.1.5.

Jin, Emily, Emily Kilcrease, and Rachel Ziemba. 'A Strategic Response to China's Economic Coercion.' Center for a New American Security, 2021. https://www.cnas.org/publications/commentary/a-strategic-response-to-chinas-economic-coercion.

Joint Chiefs of Staff. 'DOD Dictionary of Military and Associated Terms (June 2018).' United States. Joint Chiefs of Staff, June 2018. https://www.hsdl.org/?abstract&did=813130.

———. 'Joint Publication 3-13. Information Operations.' Accessed June 17, 2022. https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_13.pdf.

Keršanskas, Vytautas. 'Hybrid CoE Paper 2: DETERRENCE – Proposing a More Strategic Approach to Countering Hybrid Threats.' *Hybrid CoE - The European Centre of Excellence for Countering Hybrid Threats* (blog). Accessed June 17, 2022. https://www.hybridcoe.fi/publications/hybrid-coe-paper-2-deterrence-proposing-a-more-strategic-approach-to-countering-hybrid-threats/.

Klimburg, Alexander. 'Mixed Signals: A Flawed Approach to Cyber Deterrence.' *Global Politics and Strategy* 62, no. 1 (January 2, 2020): 107–30. https://doi.org/10.1080/00396338.2020.1715071.

———. *The Darkening Web: The War for Cyberspace*. Penguin Press, 2017.

———. 'The Whole of Nation in Cyberpower.' *Georgetown Journal of International Affairs*, 2011, 171–79. https://www.jstor.org/stable/43133826.

Kroenig, Matthew, and Barry Pavel. 'How to Deter Terrorism.' *The Washington Quarterly* 35, no. 2 (April 2012): 21–36. https://doi.org/10.1080/0163660X.2012.665339.

Kuo, Raymond. 'Secrecy among Friends: Covert Military Alliances and Portfolio Consistency.' *Journal of Conflict Resolution* 64, no. 1 (January 1, 2020): 63–89. https://doi.org/10.1177/0022002719849676.

Kuok, Lynn. 'How China's Actions in the South China Sea Undermine the Rule of Law.' *Brookings* (blog), November 18, 2019. https://www.brookings.edu/research/how-chinas-actions-in-the-south-china-sea-undermine-the-rule-of-law/.

Lange-Ionatamisvili, Elina, Nino Bolkvadze, Ketevan Chachava, Gogita Ghvedashvili, James McMillan, Nana Kalandarishvili, Natia Kuprashvili, Tornike Sharashenidze, and Tinatin Tsomaia. 'Georgia's Information Environment through the Lens of Russia's Influence.' NATO Strategic Communications Centre of Excellence, 2021. https://stratcomcoe.org/publications/georgias-information-environment-through-the-lens-of-russias-influence/212.

Laskai, Lorand. 'A New Old Threat: Countering the Return of Chinese Industrial Cyber Espionage.' Council on Foreign Relations. Accessed June 8, 2022. https://www.cfr.org/report/threat-chinese-espionage.

Levy, Jack S. 'The Diversionary Theory of War: A Critique.' In *Handbook of War Studies (Routledge Revivals)*, edited by Manus I. Midlarsky, 259–88. Accessed June 17, 2022. http://fas-polisci.rutgers.edu/levy/articles/Levy%20-%20Diversionary%20theory.pdf.

Lewis, James A. 'Cross-Domain Deterrence and Credible Threats.' Center for Strategic and International Studies, 2010. https://www.csis.org/analysis/cross-domain-deterrence-and-credible-threats.

Lilli, Eugenio. 'Redefining Deterrence in Cyberspace: Private Sector Contribution to National Strategies of Cyber Deterrence.' *Contemporary Security Policy* 42, no. 2 (2021): 163–88. https://doi.org/10.1080/13523260.2021.1882812.

Limnell, Jarno. 'Hybrid CoE Strategic Analysis 6: Countering Hybrid Threats: Role of Private Sector Increasingly Important – Shared Responsibility Needed.' Hybrid CoE. Accessed June 10,

2022. https://www.hybridcoe.fi/publications/hybrid-coe-strategic-analysis-6-countering-hybrid-threats-role-of-private-sector-increasingly-important-shared-responsibility-needed/.

Mahnken, Thomas G. 'Cost-Imposing Strategies: A Brief Primer.' Center for a New American Security, 2014. https://www.jstor.org/stable/resrep06137.

Mallory, King. 'New Challenges in Cross-Domain Deterrence.' RAND Corporation, April 12, 2018. https://www.rand.org/pubs/perspectives/PE259.html.

Manzo, Vincent A. 'After the First Shots: Managing Escalation in Northeast Asia.' *Joint Force Quarterly* 77. Accessed June 21, 2022. https://ndupress.ndu.edu/Media/News/News-Article-View/Article/581877/after-the-first-shots-managing-escalation-in-northeast-asia/.

Mayer Brown LLP. 'USTR Releases Annual Report to Congress on China's WTO Compliance | Perspectives & Events | Mayer Brown.' Accessed May 16, 2022. https://www.mayerbrown.com/en/perspectives-events/publications/2022/03/ustr-releases-annual-report-to-congress-on-chinas-wto-compliance.

Mazarr, Michael J. 'Understanding Deterrence.' RAND Corporation, April 19, 2018. https://www.rand.org/pubs/perspectives/PE295.html.

———. 'Understanding Deterrence.' In *NL ARMS Netherlands Annual Review of Military Studies 2020: Deterrence in the 21st Century—Insights from Theory and Practice*, edited by Frans Osinga and Tim Sweijs, 13–28. NL ARMS. The Hague: T.M.C. Asser Press, 2021. https://doi.org/10.1007/978-94-6265-419-8_2.

Mazarr, Michael J., Arthur Chan, Alyssa Demus, Bryan Frederick, Alireza Nader, Stephanie Pezard, Julia A. Thompson, and Elina Treyger. 'What Deters and Why: Exploring Requirements for Effective Deterrence of Interstate Aggression.' RAND Corporation, November 20, 2018. https://www.rand.org/pubs/research_reports/RR2451.html.

McDermott, Roger. 'The Kremlin's Strategy on Ukraine and Conflict De-Escalation.' *The Jamestown Foundation - Eurasia Daily Monitor* (blog). Accessed June 14, 2022. https://jamestown.org/program/the-kremlins-strategy-on-ukraine-and-conflict-de-escalation/.

Meer, Sico van der. 'Defence, Deterrence, and Diplomacy: Foreign Policy Instruments to Increase Future Cybersecurity.' In *Securing Cyberspace: International and Asian Perspectives*. Pentagon Press, 2016. https://www.clingendael.org/sites/default/files/2016-02/book_securing-cyberspace-chapter_July2016.pdf.

'MINDEF Singapore.' Accessed May 10, 2022. https://www.mindef.gov.sg/web/portal/mindef/defence-matters/defence-topic/defence-topic-detail/defence-policy-and-diplomacy.

Ministry of Defence. 'Deterrence: The Defence Contribution (JDN 1/19).' GOV.UK. Accessed June 17, 2022. https://www.gov.uk/government/publications/deterrence-the-defence-contribution-jdn-119.

Monaghan, Sean. 'Countering Hybrid Warfare: So What for the Future Joint Force?' *PRISM* 8, no. 2 (n.d.): 17.

———. 'Hybrid CoE Paper 12: Deterring Hybrid Threats: Towards a Fifth Wave of Deterrence Theory and Practice.' *Hybrid CoE - The European Centre of Excellence for Countering Hybrid Threats* (blog). Accessed June 17, 2022. https://www.hybridcoe.fi/publications/hybrid-coe-paper-12-deterring-hybrid-threats-towards-a-fifth-wave-of-deterrence-theory-and-practice/.

Morgan, Patrick M. *Deterrence Now*. Cambridge Studies in International Relations. Cambridge: Cambridge University Press, 2003. https://doi.org/10.1017/CBO9780511491573.

Morris, Lyle, Michael J. Mazarr, Jeffrey Hornung, Stephanie Pezard, Anika Binnendijk, and Marta Kepe. *Gaining Competitive Advantage in the Gray Zone: Response Options for Coercive Aggression Below the Threshold of Major War*. RAND Corporation, 2019. https://doi.org/10.7249/RR2942.

'MSB – The Swedish Civil Contingencies Agency.' Accessed June 2, 2022. https://www.msb.se/en/.

N, P, and R. 'The Effects of Sanctions Targeting Russian Oligarchs.' *NPR*, March 6, 2022, sec. Europe. https://www.npr.org/2022/03/06/1084834279/the-effects-of-sanctions-targeting-russian-oligarchs.

Nakashima, Ellen. 'At Nations' Request, U.S. Cyber Command Probes Foreign Networks to Hunt Election Security Threats.' *Washington Post*. Accessed May 4, 2022. https://www.washingtonpost.com/world/national-security/at-nations-request-us-cyber-command-probes-foreign-networks-to-hunt-election-security-threats/2019/05/07/376a16c8-70f6-11e9-8be0-ca575670e91c_story.html.

NATO. 'Collective Defence - Article 5.' NATO. Accessed June 9, 2022. https://www.nato.int/cps/en/natohq/topics_110496.htm.

'NATO 2022 - Strategic Concept.' Accessed June 30, 2022. https://www.nato.int/strategic-concept/.

NATO Strategic Communications Centre of Excellence. 'Riga Stratcom Dialogue.' Accessed June 2, 2022. https://rigastratcomdialogue.org/.

Neal, John J. 'Deterrence in a Hybrid Environment | George C. Marshall European Center For Security Studies.' George C. Marshall European Center For Security Studies. Accessed June 17, 2022. https://www.marshallcenter.org/sites/default/files/files/2020-09/pC_V10N1_en_Neal.pdf.

Novosti, Ria. 'Russia Expels Dozens Of European Diplomats In Reciprocal Move.' *Radio Free Europe*, 2022. https://www.rferl.org/a/russia-expels-european-diplomats/31856907.html.

Nye, Joseph S. 'Can China Be Deterred in Cyber Space? | EastWest Institute.' Accessed June 17, 2022. https://www.eastwest.ngo/idea/can-china-be-deterred-cyber-space.

———. 'Soft Power.' *Foreign Policy* 80 (1990): 153–71. https://doi.org/10.2307/1148580.

Nyemann, Dorthe Bach, and Heine Sorensen. 'Hybrid CoE Strategic Analysis 13: Going Beyond Resilience. A Revitalised Approach to Countering Hybrid Threats.' *Hybrid CoE - The European Centre of Excellence for Countering Hybrid Threats* (blog). Accessed June 17, 2022. https://www.hybridcoe.fi/publications/hybrid-coe-strategic-analysis-13-going-beyond-resilience-a-revitalised-approach-to-countering-hybrid-threats/.

Oliver, Isabella, and Mariakarla N. Venancio. 'Understanding the Failure of the U.S. Embargo on Cuba.' WOLA, 2022. https://www.wola.org/analysis/understanding-failure-of-us-cuba-embargo/.

'Operation Aurora - an Overview | ScienceDirect Topics.' Accessed June 10, 2022. https://www.sciencedirect.com/topics/computer-science/operation-aurora.

Pamment, James, and Anneli Kimber Lindwall. 'Fact Checking and Debunking.' NATO Strategic Communications Centre of Excellence. Accessed June 2, 2022. https://stratcomcoe.org/publications/fact-checking-and-debunking/8.

Pamment, James, Vladimir Sazonov, Francesca Granelli, Sean Aday, Maris Andzans, Una Berzina-Cerenkova, John-Paul Gravelines, et al. 'Hybrid Threats: Confucius Institutes.' NATO Strategic Communications Centre of Excellence. Accessed May 16, 2022. https://stratcomcoe.org/publications/hybrid-threats-confucius-institutes/88.

Paul, Christopher. *Strategic Communication: Origins, Concepts, and Current Debates*. Santa Barbara, CA: Praeger, 2011.

Paul, Christopher, Colin P. Clarke, Bonnie L. Triezenberg, David Manheim, and Bradley Wilson. 'Improving C2 and Situational Awareness for Operations in and Through the Information Environment.' RAND Corporation, November 1, 2018. https://www.rand.org/pubs/research_reports/RR2489.html.

Peksen, Dursun. 'When Do Imposed Economic Sanctions Work? A Critical Review of the Sanctions Effectiveness Literature.' *Defence and Peace Economics* 30, no. 6 (September 19, 2019): 635–47. https://doi.org/10.1080/10242694.2019.1625250.

Pezard, Stephanie, and Ashley L. Rhoades. 'What Provokes Putin's Russia?: Deterring Without Unintended Escalation.' RAND Corporation, January 29, 2020. https://www.rand.org/pubs/perspectives/PE338.html.

Pijpers, Peter B. M. J., and P. a. L. Ducheine. ''If You Have a Hammer…' Reshaping the Armed Forces' Discourse on Information Maneuver.' SSRN Scholarly Paper. Rochester, NY, November 1, 2021. https://doi.org/10.2139/ssrn.3954218.

Pollpeter, Kevin. 'Controlling the Information Domain: Space, Cyber, and Electronic Warfare.' *The National Bureau of Asian Research (NBR)* (blog). Accessed April 29, 2022. https://www.nbr.org/publication/controlling-the-information-domain-space-cyber-and-electronic-warfare/.

Representative, Office of the United States Trade. 'Investigation: Technology Transfer, Intellectual Property, and Innovation.' United States Trade Representative. Accessed June 17, 2022. http://ustr.gov/issue-areas/enforcement/section-301-investigations/section-301-china/investigation.

Riordan, Shun. 'The EU Is Wasting Money on Strategic Communication.' *USC Center on Public Diplomacy* (blog), December 6, 2017. https://uscpublicdiplomacy.org/blog/eu-wasting-money-strategic-communication.

Ruhle, Michael. 'The Nine Commandments on Countering Hybrid Threats | Internationale Politik Quarterly.' Internationale Politik Quarterly. Accessed May 12, 2022. https://ip-quarterly.com/en/nine-commandments-countering-hybrid-threats.

'Russia's Ill-Fated Invasion of Ukraine: Lessons in Modern Warfare.' Accessed June 24, 2022. https://www.csis.org/analysis/russias-ill-fated-invasion-ukraine-lessons-modern-warfare.

Sakellariadis, John. 'How the Justice Department Is Stepping up Its Efforts To Indict State-Sponsored Hackers.' *The Record by Recorded Future* (blog), February 3, 2021. https://therecord.media/how-the-justice-department-is-stepping-up-its-efforts-to-indict-state-sponsored-hackers/.

Salminen, Pertti. 'Finland's Comprehensive and Military Defence Doctrines Responding to Emerging Threats and New Technologies,' 2011. https://www.osce.org/fsc/78104.

Sanger, David E., and Nicole Perlroth. 'U.S. Escalates Online Attacks on Russia's Power Grid - The New York Times.' *New York Times*, 2019. https://www.nytimes.com/2019/06/15/us/politics/trump-cyber-russia-grid.html.

Sartori, Anne E. *Deterrence by Diplomacy*, 2007. https://press.princeton.edu/books/paperback/9780691134000/deterrence-by-diplomacy.

Savolainen, Jukka, Terry D. Gill, Valentin J. Schatz, Lauri M. Ojala, Tadas Jakstas, and Pirjo Kleemola-Juntunen. *Handbook on Maritime Hybrid Threats: 10 Scenarios and Legal Scans: Working Paper*. Edited by Tiia Lohela and Valentin J. Schatz. Helsinki: European Centre of Excellence for Countering Hybrid Threats, 2019. https://www.hybridcoe.fi/publications/hybrid-coe-working-paper-5-handbook-on-maritime-hybrid-threats-10-scenarios-and-legal-scans/.

Schaub, Gary. 'Deterrence, Compellence, and Prospect Theory.' *Political Psychology* 25, no. 3 (2004): 389–411. https://www.jstor.org/stable/3792549.

———. 'When Is Deterrence Necessary? Gauging Adversary Intent.' *Strategic Studies Quarterly* 3 (January 1, 2009): 27.

Schaus, John. 'What Works: Countering Gray Zone Coercion.' Center for Strategic and International Studies. Accessed June 17, 2022. https://www.csis.org/analysis/what-works-countering-gray-zone-coercion.

Schelling, Thomas C. *Arms and Influence*. Yale University Press, 1966. https://www.jstor.org/stable/j.ctt5vm52s.

———. *The Strategy of Conflict: With a New Preface by the Author*. Harvard University Press, 1980.

———. 'The Threat That Leaves Something to Chance.' RAND Corporation, 1959. https://www.rand.org/pubs/historical_documents/HDA1631-1.html.

Schwenka, Madi, and Kiera Welch. 'Perceptions, Assumptions, and Options in Deterrence Strategy and Response Policy,' n.d., 17.

Seals, Aaron. 'Dismantling the WTO: The United States' Battle Against World Trade.' *University of Miami Business Law Review* 28, no. 1 (2019): 22.

Sheppard, Lindsey R., and Matthew Conklin. 'Warning for the Gray Zone.' Center for Strategic and International Studies, 2019. https://www.csis.org/analysis/warning-gray-zone.

Snyder, Glenn H. *Deterrence and Defense*. *Deterrence and Defense*. Princeton University Press, 2015. https://doi.org/10.1515/9781400877164.

Sperandei, Maria. 'Bridging Deterrence and Compellence: An Alternative Approach to the Study of Coercive Diplomacy.' *International Studies Review* 8, no. 2 (2006): 253–80. https://www.jstor.org/stable/3880225.

Speranza, Lauren. 'A Strategic Concept for Countering Russian and Chinese Hybrid Threats.' Atlantic Council of the United States, 2020. https://www.atlanticcouncil.org/wp-content/uploads/2020/07/Strategic-Concept-for-Countering-Russian-and-Chinese-Hybrid-Threats-Web.pdf.

Sweijs, Tim, and Samuel Zilincik. 'The Essence of Cross-Domain Deterrence.' In *NL ARMS Netherlands Annual Review of Military Studies 2020*, edited by Tim Sweijs and Frans Osinga, 129–58. NL ARMS. Springer, n.d. https://link.springer.com/chapter/10.1007/978-94-6265-419-8_8.

Sweijs, Tim, Samuel Zilincik, Frank Bekkers, and Rick Meessen. 'A Framework for Cross-Domain Strategies Against Hybrid Threats.' HCSS. Accessed June 17, 2022. https://hcss.nl/report/a-framework-for-cross-domain-strategies-against-hybrid-threats/.

Szymański, Piotr. 'New Ideas for Total Defence. Comprehensive Security in Finland and Estonia.' Warszawa: Ośrodek Studiów Wschodnich im. Marka Karpia, 2020.

Tabahriti, Sam. 'Oligarch Sanctions Were Essentially a Good Idea but They Won't Sway Putin — and the Aftermath Is Uncertain, Says Expert.' Business Insider. Accessed May 15, 2022. https://www.businessinsider.com/sanctions-oligarchs-good-idea-not-affect-putin2022-4.

Cybersecurity Tech Accord. 'Tech Accord.' Accessed June 10, 2022. https://cybertechaccord.org/.

The Week. 'Do Economic Sanctions Actually Work?' *The Week UK* (blog). Accessed June 9, 2022. https://www.theweek.co.uk/88349/fact-check-do-economic-sanctions-actually-work.

Tidy, Joe. '74% of Ransomware Revenue Goes to Russia-Linked Hackers.' *BBC News*, February 14, 2022, sec. Technology. https://www.bbc.com/news/technology-60378009.

Treverton, Gregory F., Andrew Thvedt, Alicia R Chen, Kathy Lee, and Madeline McCue. 'Addressing Hybrid Threats.' Swedish Defence University, 2018.

'United States Cyber Command, 'Achieve and Maintain Cyberspace Superiority: Command Vision for US Cyber Command,' Released March 23, 2018, (12 Pages), Unclassified | National Security Archive.' Accessed June 15, 2022. https://nsarchive.gwu.edu/document/16477-united-states-cyber-command-achieve-and-maintain.

United States Joint Forces Command. 'Commander's Handbook for Strategic Communication and Communication Strategy.' UNITED STATES JOINT FORCES COMMAND NORFOLK VA, June 24, 2010. https://apps.dtic.mil/sti/citations/ADA525371.

U.S. Department of Defense. 'Strategic Communication Joint Integrating Concept,' 2009.

USAID. 'Multi-Stakeholder Initiatives with the Private Sector.' US

Väljataga, Ann. 'Back to Square One? The Fifth UN GGE Fails to Submit a Conclusive Report at the UN General Assembly.' *NATO Cooperative Cyber Defence Centre of Excellence* (blog). Accessed June 13, 2022. https://ccdcoe.org/incyder-articles/back-to-square-one-the-fifth-un-gge-fails-to-submit-a-conclusive-report-at-the-un-general-assembly/.

Vuori, Juha A. 'Deterring Things with Words: Deterrence as a Speech Act1.' *New Perspectives* 24, no. 2 (September 1, 2016): 23–50. https://doi.org/10.1177/2336825X1602400203.

Washington Post. 'U.S. Cyber Command Operation Disrupted Internet Access of Russian Troll Factory on Day of 2018 Midterms.' Accessed June 8, 2022. https://www.washingtonpost.com/world/national-security/us-cyber-command-operation-disrupted-internet-access-of-russian-troll-factory-on-day-of-2018-midterms/2019/02/26/1827fc9e-36d6-11e9-af5b-b51b7ff322e9_story.html.

Wasser, Becca, Ben Connable, Anthony Atler, James Sladden, Arroyo Center, Arroyo Center, and United States Army Special Operations Command, eds. *Comprehensive Deterrence Forum: Proceedings and Commisioned Papers*. Conference Proceedings, CF-345-A. Santa Monica, Calif: RAND Corporation, 2018.

Welle (www.dw.com), Deutsche. 'Taiwan Opens Representative Office in Lithuania | DW | 18.11.2021.' DW.COM. Accessed June 10, 2022. https://www.dw.com/en/taiwan-opens-representative-office-in-lithuania/a-59853874.

Wigell, Mikael. 'Democratic Deterrence: How to Dissuade Hybrid Interference.' *The Washington Quarterly* 44, no. 1 (January 2, 2021): 49–67. https://doi.org/10.1080/0163660X.2021.1893027.

Wigell, Mikael, Harri Mikkola, and Tapio Juntunen. 'Best Practices in the Whole-of-Society Approach in Countering Hybrid Threats,' n.d., 60.

Wike, Richard, Katie Simmons, Bruce Stokes, and Janell Fetterolf. 'Globally, Broad Support for Representative and Direct Democracy.' *Pew Research Center's Global Attitudes Project* (blog), October 16, 2017. https://www.pewresearch.org/global/2017/10/16/globally-broad-support-for-representative-and-direct-democracy/.

Williams, Rachel. 'Lessons In Deterrence From U.S. Foreign Policy In Iraq, 1982 2003,' n.d., 103.

Wiśniewski, Rafał. 'Economic Sanctions as a Tool of China's Hybrid Strategies.' *Polish Political Science Yearbook* 50, no. 1 (December 31, 2021): 1–13. https://czasopisma.marszalek.com.pl/10-15804/ppsy/1021-ppsy-vol-50/ppsy-50-all/7103-ppsy202133.

Wright, Thomas. 'Democrats Must Act Now to Deter Foreign Interference in the 2020 Election.' *Brookings* (blog), October 4, 2019. https://www.brookings.edu/blog/order-from-chaos/2019/10/04/democrats-must-act-now-to-deter-foreign-interference-in-the-2020-election/.

Zumbrun, Josh, and Bob Davis. 'China Trade War Didn't Boost U.S. Manufacturing Might.' *Wall Street Journal*, October 25, 2020, sec. Politics. https://www.wsj.com/articles/china-trade-war-didnt-boost-u-s-manufacturing-might-11603618203.

The Hague Centre
for Strategic Studies

HCSS
Lange Voorhout 1
2514 EA Hague

Follow us on social media:
@hcssnl

The Hague Centre for Strategic Studies
Email: info@hcss.nl
Website: www.hcss.nl