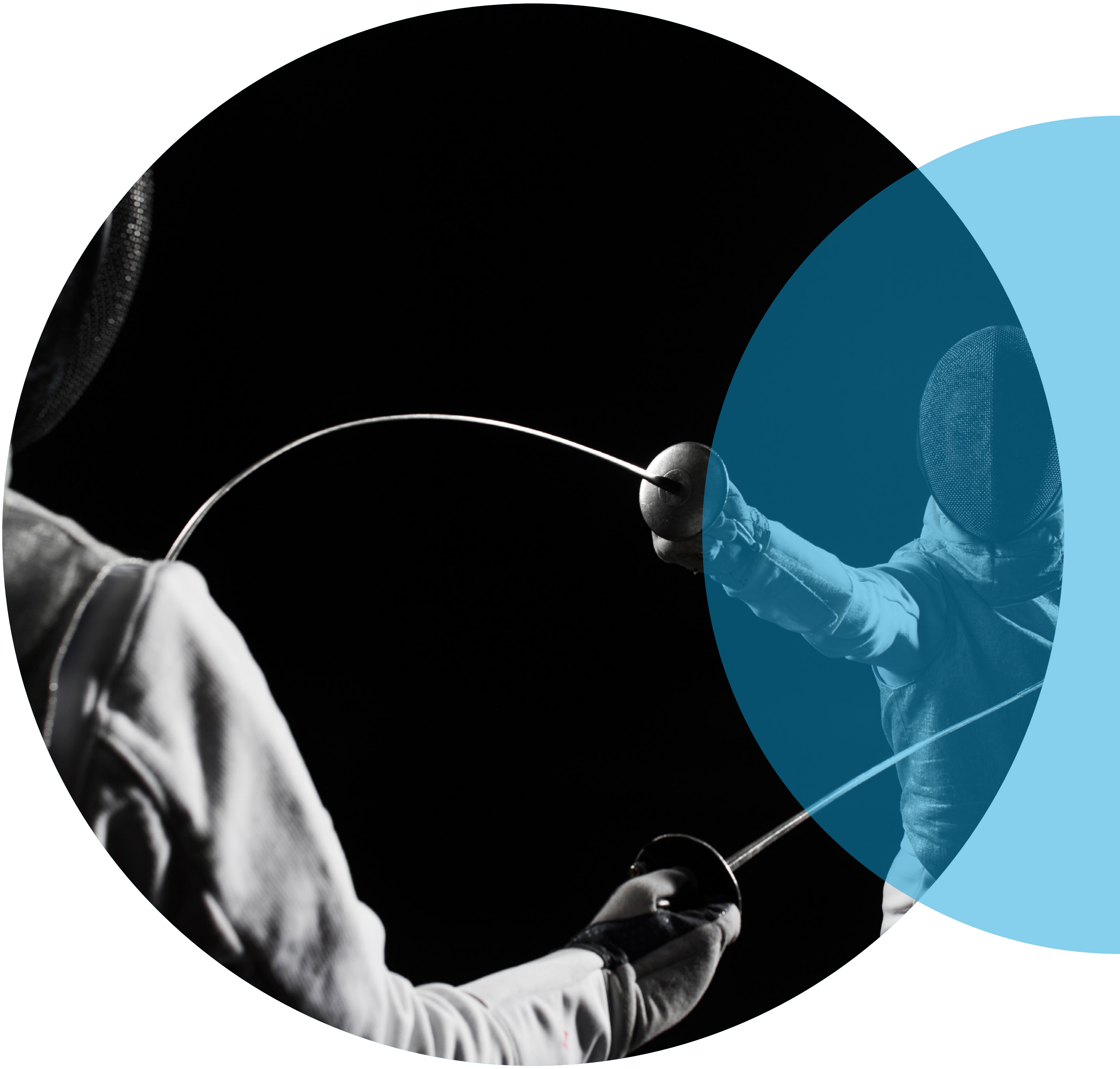
Hybrid CoE Paper 12

Deterring hybrid threats: Towards a fifth wave of deterrence theory and practice



Hybrid CoE

Sean Monaghan – March 2022

Cover photo: Dmytro Kapitonenko / shutterstock.com

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

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

ISBN (web) 978–952–7472–28–6
ISBN (print) 978–952–7472–29–3
ISSN 2670–2053

March 2022

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

The responsibility for the views expressed ultimately rests with the authors.

Contents

Executive summary

This Hybrid CoE Paper looks again at theory and practice to restore the foundations of deterrence against hybrid threats below the threshold of war. It also looks to the future of hybrid threats and new horizons in deterrence – including the prospect of a post-modern, fifth wave of deterrence theory and practice.

Hybrid threats combine modern tools of statecraft to seek gains while avoiding reprisal. Hybrid threats are not new – they exploit classical principles of strategy such as winning without fighting, the indirect approach, measures short of war and salami-tactics. But they are newly relevant to strategic challenges in the years ahead. Future trends in power, interdependence and technology suggest more motivated revisionist actors will have more access to means that can target more vulnerabilities more cost effectively, using tools and domains of action which cover the full spectrum of modern domestic and international life.

The rise of hybrid threats can be traced to both successes and failures of deterrence. While deterrence has often succeeded in dissuading revisionist actors from resorting to conventional armed aggression, it has also failed to prevent hostile state activity – in the form of hybrid threats.

Hybrid threats undermine the foundations of deterrence – capability, credibility and communication – in specific ways. This paper develops several insights and principles to help restore these foundations by refining and applying classical principles such as absolute vs restrictive deterrence, general vs. immediate deterrence, direct vs extended deterrence, denial vs.

punishment and deterrence vs compellence. It also offers a framework for applying these principles to deter hybrid threats.

This paper also points to four new horizons for further development and research. These include the role of military force in deterring hybrid threats, going beyond deterrence, the evolution of hybrid threats and the future of deterrence – on which **the prospect of a post-modern, fifth wave of deterrence theory and practice is outlined.** This idea widens the concept of deterrence across the breadth of hybrid threats, including the established literature on cross-domain deterrence. Such a fifth wave has elements of continuity with previous waves – such as psychology, the role of military force, the centrality of state-actors – but also new elements, including the predominance of non-military hybrid threats that span government and society, unprecedented complexity, variety and connectedness, a large sub-state component, and a shift away from punishment towards denial through resilience.

Future tools of deterrence will be wielded less by the military and government and more by the whole of society, woven into the fabric of everyday life. Just as some have described the coming era as involving the 'weaponisation of everything', deterrence in the era of hybrid threats may become a post-modern case of the deterrence of everything. Looking further into the future, the truly revolutionary implications of AI may invite a sixth wave of deterrence theory and practice – when the essence of deterrence moves beyond the manipulation of human decisions to the inscrutable logic of intelligent machines.

Acknowledgements

This paper is indebted to:

- the MCDC Countering Hybrid Warfare project and everyone who participated in it (many of these ideas were born there);
- the Dstl Head Office Decision Making project (including Aimee Feeney, Sam Guthrie, Dr Adam Lyons, Ben Millman, Hamzah Muneer, Dr Gordon Niven, Dan Sowik and Nik Taylor);
- the Hybrid CoE team who reviewed a draft of this paper – particularly Viktorija Rusinaite and Stuart Mackie, who sponsored the project and provided wise counsel throughout.

1. Introduction

Deterrence is the foundation of any strategy to counter hybrid threats. This is why the Deterrence Playbook published by the European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE) in 2020 is such an important resource. The Playbook was based on the simple insight that "the rich theory and practice of deterrence could be applied to efforts to counter hybrid threats".[1]

This paper seeks to build on those foundations to develop further insights and principles for deterring hybrid threats. Hybrid CoE's Playbook was practical in nature (hence the term 'playbook'), whereas this paper is conceptual. The aim is to identify insights from deterrence theory which might improve the prospects for deterring hybrid threats. These insights can be used and developed further by communities of best practice like Hybrid CoE, and put into action.

The paper proceeds in three parts. It first recaps the basic tenets of hybrid threats and deterrence – including the foundations of deterrence: the 'three Cs' of capability, credibility and communication. Next, in light of the unique challenges posed by hybrid threats, the rich history and recent developments in deterrence theory and practice are examined. Several insights are developed which might reinforce the foundations of deterrence against hybrid threats. Finally, the paper looks to new horizons in deterring hybrid threats – particularly the prospect of a post-modern, 'fifth wave' of deterrence theory and practice.

[1] Hybrid CoE, 'Hybrid CoE launches a playbook on hybrid deterrence', News, 9 March 2020, https://www.hybridcoe.fi/news/hybrid-coe-launches-a-playbook-on-hybrid-deterrence/; Vytautas Keršanskas, 'Deterrence: Proposing a more strategic approach to countering hybrid threats', (Hybrid CoE Paper 2, March 2020), 6, https://www.hybridcoe.fi/wp-content/uploads/2020/07/Deterrence_public.pdf. [All links were last accessed on 4 March 2022.]

2. What are hybrid threats?

2.1. The hybrid threat landscape

Hybrid CoE uses four pillars to help understand the hybrid threat landscape.[2]

Actors

The shifting balance of global and regional power is producing more state actors that are unsatisfied with their position in a changing world. While motivated to seek actual (e.g. territory or assets) or intangible (e.g. status or reputation) gains, they are also sufficiently entangled in the status quo to rule out acting definitively to break free.[3] Such motivated-but-constrained states use hybrid threats to pursue strategies of measured revisionism.[4] While non-state actors may feature as threat actors and proxies in the context of state aggression, they are rarely entangled or constrained enough to resort to hybrid threats themselves. Instead they rely on more revolutionary (violent) means.[5]

Tools and domains

The globalized, interconnected and digitized modern world provides plenty of opportunities for motivated revisionists to cause or threaten harm to create leverage.[6] The tools used and domains of action cover the full spectrum of modern domestic and international life. Many of these offer options to cultivate ambiguity about actors or actions – particularly in the digital realm. Such a post-modern approach to conflict was predicted by futurists Alvin and Heidi Toffler in the 1990s, who said we make war how we make money.[7]

Phases

Hybrid threat actors operate in the grey zone between peace and war. Hybrid CoE divides this dynamic spectrum of action into three types, shown in Figure 1 below.

[2] G. Giannopoulos, H. Smith & M. Theocharidou, 'The Landscape of Hybrid Threats: A Conceptual Model – Public Version', (The European Commission and the European Centre of Excellence for Countering Hybrid Threats, 26 November 2020), https://www.hybridcoe.fi/wp-content/uploads/2021/02/conceptual_framework-reference-version-shortened-good_cover_-_publication_office.pdf.

[3] Entanglement is either 'hard' (e.g. dissuaded by the threat of punishment) or 'soft' (e.g. incentivized by the benefits of globalized trade and interdependence).

[4] Michael J. Mazarr, 'Mastering the Gray Zone: Understanding a Changing Era of Conflict', (Strategic Studies Institute and U.S. Army War College Press, December 2015), 22, https://publications.armywarcollege.edu/pubs/2372.pdf.

[5] Including hybrid warfare, which is not the subject of this paper. See: Frank G. Hoffman, 'Examining Complex Forms of Conflict: Gray Zone and Hybrid Challenges', *PRISM Journal*, Volume 7, Issue 4 (2018), https://cco.ndu.edu/news/article/1680696/examining-complex-forms-of-conflict-gray-zone-and-hybrid-challenges/; and Sean Monaghan, 'Countering Hybrid Warfare: So What for the Joint Force?', *PRISM Journal*, Volume 8, Issue 2 (2019): 83–88, https://ndupress.ndu.edu/Portals/68/Documents/prism/prism_8-2/PRISM_8-2_Monaghan.pdf. Note: Non-state actors may be used as hybrid threat tools, for example private militias or cyber criminals.

[6] For lists of potential instruments used to construct hybrid threats, see: Giannopoulos, Smith & Theocharidou, 'The Landscape of Hybrid Threats', 33–35; Monaghan, 'Countering Hybrid Warfare', 89; S. Aday et al., 'Hybrid Threats: A Strategic Communications Perspective', (NATO StratCom CoE, 2019), https://stratcomcoe.org/publications/hybrid-threats-a-strategic-communications-perspective/79.

[7] In their 1993 book *War and Anti-War*, Alvin and Heidi Toffler describe how, as the global economy evolves, so do the prevalent forms of war. Based on the insight that "the way we make war reflects the way we make wealth", they suggest 'third wave' economies – i.e. those increasingly dependent on information rather than raw materials and physical labour – will breed third wave 'war-forms'. See: Alvin and Heidi Toffler, *War and anti-war: survival at the dawn of the twenty-first century* (Little Brown and Company, 1993).

Figure 1: Hybrid threat phases, increasing in intensity from left to right.[8]

Hybrid threat phase:	Priming	Destabilisation	Coercion
Description:	Efforts to interfere and influence in order to shape, precondition and obscure.	Operations or campaigns to influence and achieve goals which build on the effect achieved and information gathered in the priming phase.	Destabilisation operations and campaigns with the addition of coercive military threats or 'minor incursions'.

Another way of viewing this spectrum is through the severity or intensity of hybrid threats. RAND suggests three types of 'grey zone aggression' on this basis, shown in Figure 2 below.[9]

Figure 2: Hybrid threat severity, increasing in intensity from left to right.

Hybrid threat severity:	Persistent	Moderate	Aggressive
Description:	Broad-based, low-level, non-military actions with hazy attribution that don't clearly violate international laws and norms. Very difficult to deter given the persistence and low level of interests engaged.	Direct, attributable, coercive action through (mostly) non-military means which exploits legal grey areas. Difficult to deter as it falls below conventional threshoulds and can occur with little-to-no warning.	Direct, threatening, attributable quasi-military or military action in violation of international laws and norms. Can be deterred in advance with warning

[8] Giannopoulos et al., 'The Landscape of Hybrid Threats', 11.

[9] Michael J. Mazarr et al., 'What Deters and Why: Applying a Framework to Assess Deterrence of Gray Zone Aggression', Research Report (RAND, 2021), https://www.rand.org/pubs/research_reports/RR3142.html.

2.2. Seven features of hybrid threats

Hybrid threats create a defender's dilemma

Hybrid threats combine modern tools of statecraft to seek gains while avoiding reprisal.[10] They do so by presenting the target state with a dilemma: whether or not to escalate in response to a 'minor incursion'.[11] This is known as the defender's dilemma.[12]

Hybrid threats are not new – but they are relevant

Hybrid threats are not new. They exploit classical principles of strategy such as winning without fighting, the indirect approach, measures short of war and salami slicing tactics.[13] But they are newly relevant to the strategic challenges of the coming decades. The preponderance of power amongst the status quo nations, the nuclear 'balance of terror' and the incentives of participation in the globalized economy have contributed to the emergence of hybrid threats.[14] Future trends in power, interdependence and technology suggest that more revisionist actors will have more access to means that can target more vulnerabilities more cost effectively.[15]

Hybrid threats exist on a continuum of conflict

Figure 3 below shows hybrid threats on a 'continuum of conflict'. It also shows the 'grey zone' between peace and war, and 'hybrid warfare' (or the admixture of violent means).

Hybrid threats exploit complexity

Exponents of hybrid threats seek new forms of leverage and power in an increasingly complex world. They exploit complexity to produce leverage efficiently (i.e. while minimizing costs or downsides). Complexity is not just a problem for early warning and detection,[16] but for strategy writ large. This is achieved through combination, synchronization, ambiguity and non-linear effects.[17] Figure 4 below shows these features through the combination of instruments of power (stars), targeted at societal vulnerabilities (sectors), combining individual effects (pentagons) to achieve a whole effect which is greater than the sum of its parts.

[10] Hybrid threats are also referred to as grey zone strategies, hybrid war, hybrid warfare, political warfare, sub-threshold, and other names. A general understanding of the concept is more useful than a strict definition. For a good recent overview, see: *The Economist*, 'What is hybrid war, and is Russia waging it in Ukraine?', 22 February 2022, https://www.economist.com/the-economist-explains/2022/02/22/what-is-hybrid-war-and-is-russia-waging-it-in-ukraine.

[11] Elisabeth Braw, 'Biden's Gray-Zone Gaffe Highlights a Real Dilemma', Defense One, 20 January 2022, https://www.defenseone.com/ideas/2022/01/bidens-gray-zone-gaffe-highlights-real-dilemma/360982/.

[12] Elisabeth Braw, *The Defender's Dilemma: Identifying and Deterring Gray-Zone Aggression* (American Enterprise Institute, 2021), https://www.aei.org/the-defenders-dilemma/.

[13] See, respectively: Sun Tzu, *The Art of War*; Basil Liddell Hart, *Strategy: The Indirect Approach*, (London, Faber, 1967 (1929), 4th Edn); George F. Kennan, *Measures Short of War: The George F. Kennan Lectures at the National War College, 1946–47*, (National Defense University Press, 1991); Thomas Schelling, *Arms and Influence*, (Yale University Press,1966).

[14] Michael J. Mazarr et al., 'Understanding the Emerging Era of International Competition', Research Report (RAND, 2018), 30, https://www.rand.org/pubs/research_reports/RR2726.html).

[15] Monaghan, 'Countering Hybrid Warfare', 86. See below for more detail on the evolution of hybrid threats.

[16] Patrick Cullen, 'Hybrid threats as a new "wicked problem" for early warning', (Hybrid CoE Strategic Analysis 8, June 2018), https://www.hybridcoe.fi/publications/hybrid-coe-strategic-analysis-8-hybrid-threats-as-a-new-wicked-problem-for-early-warning/.

[17] Sean Monaghan et al., 'MCDC Countering Hybrid Warfare Project: Countering Hybrid Warfare', (MCDC, March 2019), 13–15, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/784299/concepts_mcdc_countering_hybrid_warfare.pdf.

Figure 3: Hybrid threats on a continuum of conflict

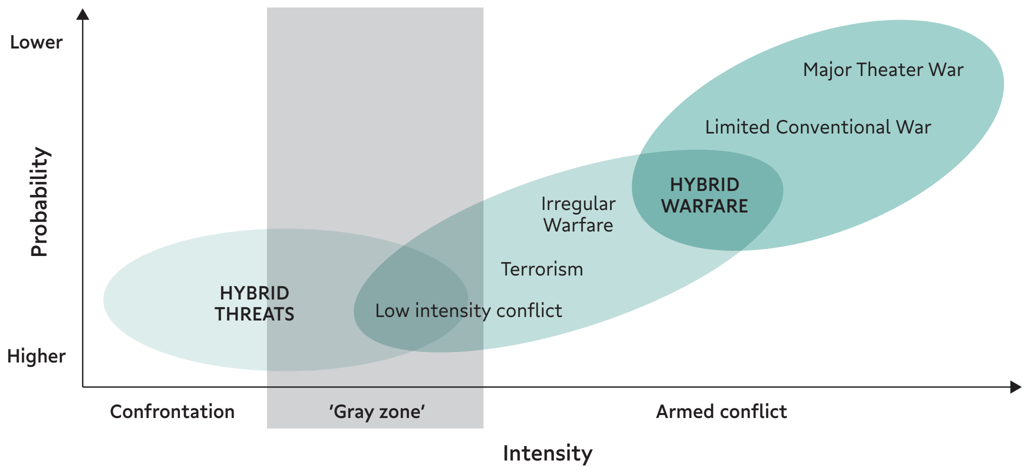
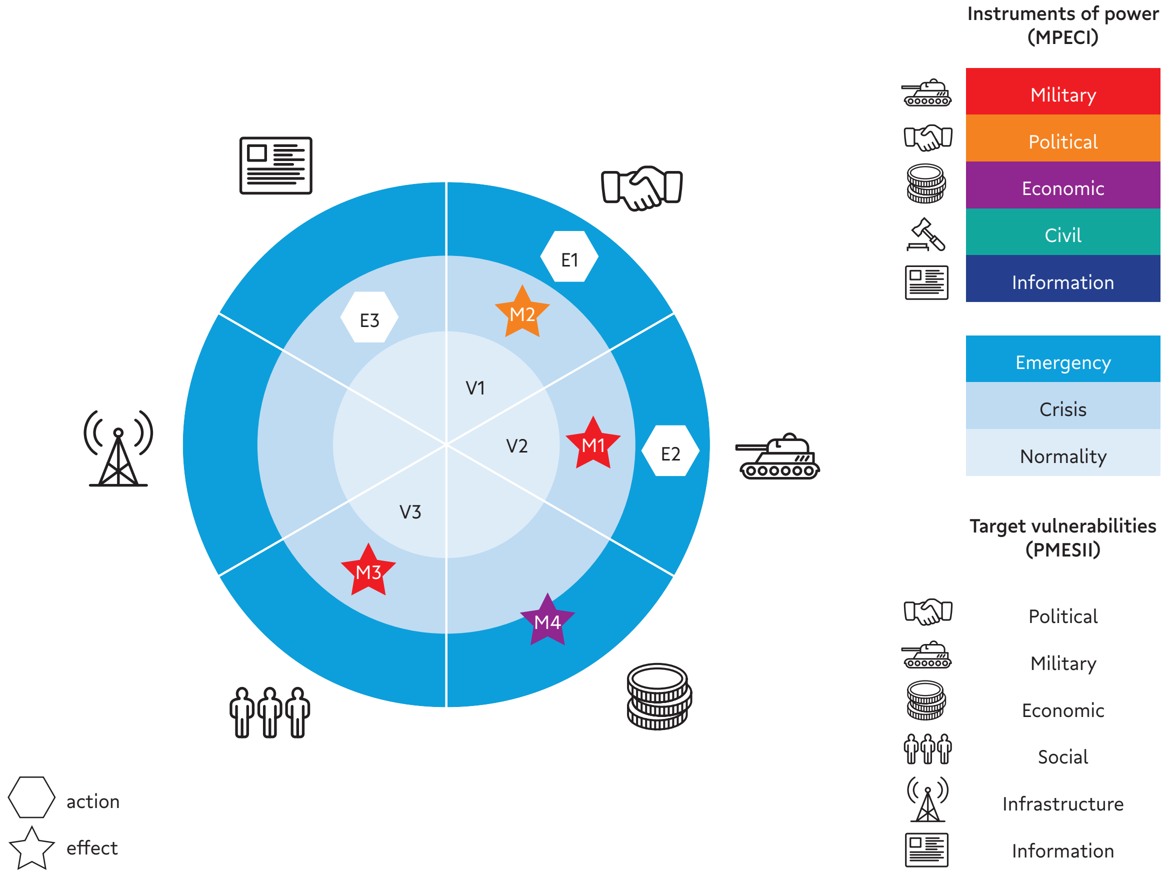


Figure 4: Visualizing hybrid threats (synchronization, ambiguity and non-linear effects).[18]



[18] Monaghan et al., 'MCDC Countering Hybrid Warfare', 15.

Hybrid threats challenge rules, order and values

The challenge of hybrid threats is also about rules, order and values. Hybrid threats are designed to circumvent, unpick and subvert the rules and norms that regulate aggression in the international system and in the domestic context. They represent an attempt to widen the scope for aggressive action and turn Clausewitz's famous dictum – that war is a continuation of politics by other means – on its head: instead, hybrid threats are the continuation of war by other (unrestricted) means, towards the "creative weaponization of everything".[19]

Ultimately, as Clausewitz observed, "the political cause of a war has a great influence on the method in which it is conducted".[20] Or, as NATO Secretary General Jens Stoltenberg put it:

> *"Hybrid is the dark reflection of our comprehensive approach. We use a combination of military and non-military means to stabilize countries. Others use it to destabilize them."*[21]

Thresholds are in the eye of the beholder

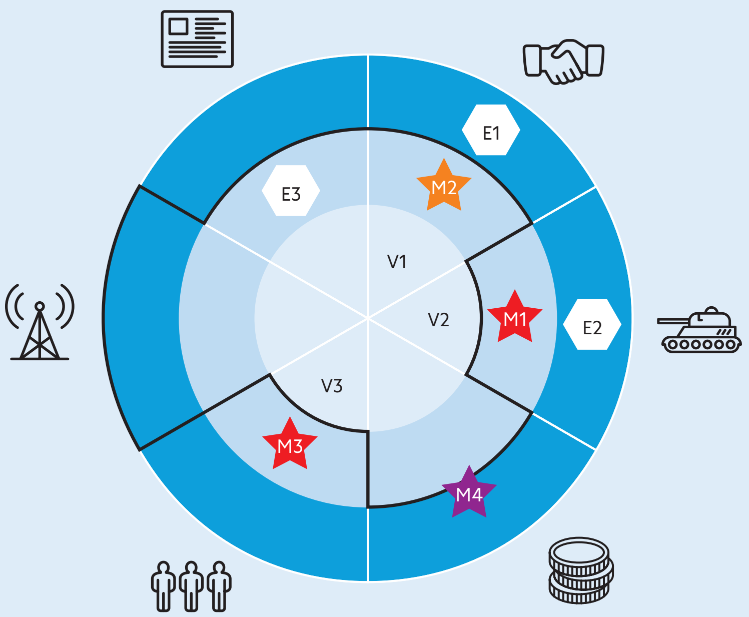
Frameworks to categorize hybrid threats (like those above) provide a helpful starting point. Yet thresholds for what matters are in the eye of the beholder. Such thresholds are a slippery concept. In practice, thresholds for preventive and retaliatory measures may only be determined post hoc due to the novelty of the threat. They may also vary depending on the nature or domain of the threat, as demonstrated in Figure 5 below.[22] Response thresholds are central to the efficacy of hybrid threats and are exploited by exponents.[23]

Hybrid threats are tools of coercion

Despite the non-violent nature of hybrid threats, they are a tool of coercion. Hence the 'hybrid' moniker, which indicates the combination of less serious threats, such as disinformation and low-level cyberattacks, with more serious ones, such as economic and military coercion through threats (whether explicit or implicit).[24] The potency of hybrid threats often depends on the prospect of escalation through the threat of

[19] For Clausewitz, see: Monaghan, 'Countering Hybrid Warfare', 88. For 'weaponization of everything', see: Nathan Freier, 'The Darker Shade of Gray: A New War Unlike Any Other', CSIS, 27 July 2018, https://www.csis.org/analysis/darker-shade-gray-new-war-unlike-any-other; Mark Galeotti, *The Weaponisation of Everything: A Field Guide to the New Way of War* (Yale University Press, 2022). It is worth noting that this point was made by Russian Chief of the General Staff Valery Gerasimov in his 2013 article (referred to by many, erroneously, as the 'Gerasimov Doctrine'). He suggested that the "very 'rules of war' have changed. The role of nonmilitary means of achieving political and strategic goals has grown". See: Valery Gerasimov (translation by Robert Coalsen), 'The Value of Science is in the Foresight', *Military Review*, Jan–Feb 2016, https://www.armyupress.army.mil/portals/7/military-review/archives/english/militaryreview_20160228_art008.pdf.
[20] Carl von Clausewitz (Michael Howard and Peter Paret), *On War*, (New York: Penguin Books, 1968), 400.
[21] Jens Stoltenberg, 'Keynote Speech', NATO HQ, 25 March 2015, http://www.nato.int/cps/en/natohq/opinions_118435.htm.
[22] For example, tolerance levels regarding public misinformation may differ from cyberattacks on critical infrastructure. For more on setting thresholds for hybrid threats, see: Monaghan et al., 'MCDC Countering Hybrid Warfare', 21.
[23] Braw, 'Biden's gray zone gaffe'.
[24] As the UK's Integrated Review puts it: "These tools of coercion and interference can also be used in 'hybrid' combination with more traditional hard power methods". Cabinet Office, 'Global Britain in a Competitive Age: the Integrated Review of Security, Defence, Development and Foreign Policy', UK HMG, 70, https://www.gov.uk/government/publications/global-britain-in-a-competitive-age-the-integrated-review-of-security-defence-development-and-foreign-policy.

Figure 5: Setting tailored, domain-specific thresholds for countering hybrid threats.[25]



hard power – without it, hybrid threats are technically still threats, just much less concerning ones.

The point is that hybrid threats cannot be considered in a vacuum, isolated from wider power dynamics. Escalation dominance creates the grey zone in the first place by dissuading more serious, armed aggression. In general terms, the escalation dominance of the status quo powers deters revisionists from resorting to armed action. More specifically, where revisionists possess local escalation dominance they may be emboldened to use more serious hybrid threats or armed action. This is where deterrence comes in.

[25] Monaghan et al., 'MCDC Countering Hybrid Warfare', 21.

3. Deterrence: the basics

In simple terms, deterrence aims to prevent a course of action by convincing a potential aggressor that the costs or consequences of their action will outweigh the potential gains. Some key principles of deterrence theory and practice are set out in Table 1 below.[26]

Table 1: Basic principles of deterrence

Deterrence principle	Focus	Description
Absolute vs. restrictive	Scope/ambition	• Restrictive deterrence seeks to minimize the negative attributes of an action – such as frequency or severity – but not deter it outright. • Absolute deterrence seeks to prevent an action from occurring absolutely, rather than restrict the occurrence or manage the consequences.
General vs. immediate	Specificity	• Immediate deterrence is undertaken through targeted actions in response to a specific, imminent threat. • General deterrence is generated over time by behaviour that portrays a clear willingness and ability to respond to hostile action. It can also decay over time if not re-established or if challenges go unmet.
Direct vs. extended	Subject	• The distinction between deterring attacks against oneself (direct deterrence) and against others (extended deterrence). • Extended deterrence applies the logic of deterrence to provide protection to a third party (e.g. NATO's Article 5 provision).
Denial vs. punishment	Mechanism	• Deterrence by denial aims to undermine the ability of the adversary to achieve their objective in the first instance – for example through increasing protection or resilience against specific forms of attack. • Deterrence by punishment aims to persuade the adversary that the costs of achieving their objective will be prohibitive by credibly threatening something of value to them.[27]
Deterrence vs compellence	Type of coercion	• Deterrence is about preventing behaviour while compellence is about changing it. This is the difference between telling a child not to do something and telling them to stop doing something. • Thomas Schelling, who originally applied this distinction to coercive strategy, considered 'ambiguous aggression' (or hybrid threats) as requiring compellence, not deterrence.[28]

[26] For some of the classic treatments of deterrence theory and practice on which this section is based, see: Patrick M. Morgan, *Deterrence: A Conceptual Analysis* (Beverly Hills: Sage Publications, 1977); Schelling, *Arms and Influence*; Glenn H. Snyder, *Deterrence and Defense: Toward a Theory of National Security* (Princeton: Princeton University Press, 1961); Lawrence Freedman, *Deterrence* (Cambridge: Polity Press, 2004); John J. Mearsheimer, *Conventional Deterrence* (Ithaca: Cornell University Press, 1983); Alexander L. George and Richard Smoke, *Deterrence in American Foreign Policy: Theory and Practice* (Columbia University Press, 1974).

[27] Snyder, *Deterrence and Defense*.

[28] Thomas C. Schelling and Anne-Marie Slaughter, *Arms and Influence* (2020 Ed), (Yale University Press, 2020), 69. See also: Sean Monaghan, 'To Change Putin's Behavior, the West Needs a New Strategy', *World Politics Review*, 9 Feb 2022, https://www.worldpoliticsreview.com/articles/30309/for-nato-deterring-a-ukraine-russia-war-isn-t-enough.

3.1. The 'three Cs' of deterrence: capability, credibility and communication

There are three core pillars to achieving effective deterrence in practice (referred to herein as the 'three Cs'):[29]

- **Capability** is the ability or technical capacity to implement deterrence measures.
- **Credibility** is the will to implement deterrence measures.
- **Communication** is the two-way understanding and perception that informs cost-benefit calculations on both sides.[30]

3.2. Why hybrid threats are difficult to deter

The rise of hybrid threats can be traced to both successes and failures of deterrence. On the one hand, deterrence has often succeeded in dissuading revisionist actors from resorting to conventional armed aggression. Yet at the same time it has often failed to dissuade those actors from conducting hostile state activity – in the form of hybrid threats. While revisionist states such as Russia, Iran and China may be dissuaded from outright conventional aggression, they are systematically employing hybrid threats below the threshold of decisive response.[31] Future trends suggest this form of aggression may well intensify (see Section 5.3.1).[32]

The conscious intent of such strategies is to undermine the core tenets of deterrence. This can be seen in Figure 6 below, which shows how hybrid threats erode the foundations of deterrence.[33]

This is why several assessments of deterrence in Europe and the Indo-Pacific suggest that the state of deterrence against hybrid threats is questionable.[34]

Hybrid CoE's *Deterrence Playbook* attempted to renew and revitalize the strategy of deterrence in the face of hybrid threats.[35] Based on the specific challenges posed by hybrid threats to deterrence, some core tenets of deterrence strategy can be revisited with this goal in mind.

[29] Robert P. Haffa Jr, 'The Future of Conventional Deterrence: Strategies for Great Power Competition', *Strategic Studies Quarterly,* Volume 12, Issue 4 (Winter 2018), 96–97.

[30] Deterrence requires altering the perception of the adversary, which also depends on understanding how that perception is formed in the first place.

[31] James M. Dubik and Nic Vincent, 'America's global competitions: the gray zone in context' (Institute for the Study of War, February 2018), https://www.understandingwar.org/sites/default/files/The%20Gray%20Zone_Dubik_2018.pdf; Michael J. Green and John Schaus, 'Countering Coercion in Maritime Asia', CSIS/Rowman & Littlefield (CSIS, 9 May 2017), https://www.csis.org/analysis/countering-coercion-maritime-asia; Michael Eisenstadt, 'Operating in the Gray Zone: Countering Iran's Asymmetric Way of War', Policy Focus (The Washington Institute for Near East Policy, 7 January 2020), https://www.washingtoninstitute.org/policy-analysis/operating-gray-zone-countering-irans-asymmetric-way-war.

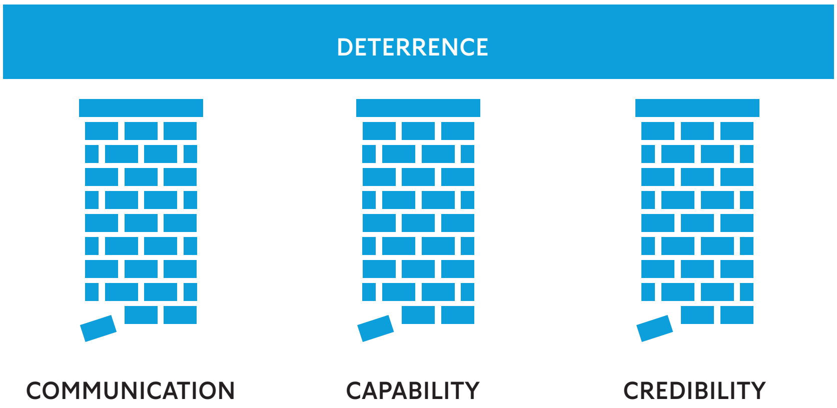
[32] UK Ministry of Defence, 'Global Strategic Trends: the future starts today (Sixth Edition)', DCDC, 2018, 132–133, https://www.gov.uk/government/publications/global-strategic-trends.

[33] Adapted from: Monaghan et al., 'MCDC Countering Hybrid Warfare', 37. See also: James Andrew Lewis, 'Cross-Domain Deterrence and Credible Threats' (CSIS, 1 July 2010), https://www.csis.org/analysis/cross-domain-deterrence-and-credible-threats; Mazarr, 'Mastering the Gray Zone'.

[34] See for example: Tim Sweijs et al., 'Strengthening deterrence against nuclear, conventional, and hybrid threats: Strengths, weaknesses, and insights for US allies in Europe and Asia' (The Hague Centre for Strategic Studies, January 2022), https://hcss.nl/report/strengthening-deterrence-nuclear-conventional-hybrid-threats/; Michael J. Mazarr et al., 'What Deters and Why'; Stacie L. Pettyjohn and Becca Wasser, 'Competing in the Gray Zone: Russian Tactics and Western Responses' (RAND US, 2019), https://www.rand.org/pubs/research_reports/RR2791.html; Ben Jensen et al., 'Shadow Risk: What Crisis Simulations Reveal about the Dangers of Deferring U.S. Responses to China's Gray Zone Campaign against Taiwan' (CSIS, 16 February 2021), https://www.csis.org/analysis/shadow-risk-what-crisis-simulations-reveal-about-dangers-deferring-us-responses-chinas-gray).

[35] This call was originally made by two Danish analysts: Heine Sørensen and Dorthe Bach Nyemann, 'Going Beyond Resilience: A revitalized approach to countering hybrid threats' (Hybrid CoE Strategic Analysis, November 2018), https://www.hybridcoe.fi/wp-content/uploads/2020/07/Strategic-analysis-13-Sorensen-Nyeman.pdf.

Figure 6: How hybrid threats undermine the foundations of deterrence.



Hybrid threat challenges:	Undermined by ambiguity and subjectivity	Undermined by the breadth and novelty of hybrid means	Undermined by targeting response thresholds and avoiding detection thresholds

4. Restoring the foundations of deterrence against hybrid threats

This section explores how the challenges posed to deterrence strategy by hybrid threats can be met. It revisits some fundamentals of deterrence and applies recent developments in the theory and practice of deterrence. Doing so reveals insights about how the foundations of deterrence might be reinforced. Each insight is designated as having the potential to strengthen one or more of the 'three Cs' – thereby reinforcing deterrence in the face of hybrid threats. This is summarized in a Table towards the end of the section, alongside a framework for deterring hybrid threats which incorporates some of these insights.

4.1. Deterrence by denial

4.1.1. Resilience is the foundation of hybrid deterrence

Deterrence by denial is regularly advocated against hybrid threats, often in the form of resilience-building measures.[36] In one survey of policy literature, around three-quarters of all measures planned or proposed were focussed on the denial of benefit.[37] Even UK military doctrine has swung towards deterrence by denial in recent years.[38]

The allure of denial through resilience is understandable. Defensive measures are generally low cost and fit well within prevalent 'risk management' paradigms of national security.[39]

[36] See for example: Tim Prior, 'Resilience: The 'Fifth Wave' in the Evolution of Deterrence', Chapter 4 in *Strategic Trends 2018*, ed. Oliver Thränert and Martin Zapfe (Center for Security Studies: ETH Zurich, 2018), https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/ST2018-06-TP.pdf); Lyle J. Morris et al., 'Gaining Competitive Advantage in the Gray Zone' (RAND, 2019), https://www.rand.org/pubs/research_reports/RR2942.html; Braw, 'The Defender's Dilemma'; Monaghan et al., 'MCDC Countering Hybrid Warfare'; Mikael Wigell et al., 'Best Practices in the whole-of-society approach in countering hybrid threats', A study requested by the INGE committee (European Parliament, May 2021), https://www.europarl.europa.eu/RegData/etudes/STUD/2021/653632/EXPO_STU(2021)653632_EN.pdf. Examples of resilience-building measures include hardening infrastructure, public education (e.g. against disinformation, or on cyber security), resource diversification, anti-corruption, etc. These approaches have been described as a form of modernized 'total defence', involving the kind of whole-of-society approaches to national resilience that were pursued by many nations during the Cold War – which have been revitalized in recent years by nations such as Sweden ('Total Defence'), Norway ('Support and Cooperation'), Finland ('Comprehensive Security'), Austria ('Comprehensive National Defence'). See: Monaghan et al., 'MCDC Countering Hybrid Warfare', 44.

[37] Monaghan et al., 'MCDC Countering Hybrid Warfare', 79–82; Albin Aronsson, 'The state of current counter hybrid warfare policy' (MCDC Information Note, 2019), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/803970/20190519-MCDC_CHW_Info_note_10-State_of_current_policy.pdf.

[38] In 2014 UK Defence Doctrine characterized deterrence as dissuading a course of action through "the threat of a military response" to "impose costs on an opponent to deter unwanted behaviour". In 2019 the UK MOD released a new deterrence doctrine which emphasized the importance of deterrence by denial and encouragement of restraint alongside deterrence by punishment to provide a more balanced approach. See: UK Ministry of Defence, 'Joint Doctrine Publication 0–01: UK Defence Doctrine (Fifth Edition)', DCDC, 62–63, https://www.gov.uk/government/publications/jdp-0-01-fourth-edition-british-defence-doctrine; and UK Ministry of Defence, 'Joint Doctrine Note 1/19: Deterrence: The defence contribution', DCDC, 2019, 40–41, https://www.gov.uk/government/publications/deterrence-the-defence-contribution-jdn-119.

[39] Aronsson, 'The state of current counter hybrid warfare policy'.

Building resilience has become a strategy in itself in an increasingly complex and unpredictable world.[40] The recent growth of cyber resilience practices and philosophy in the civil sector may also be influential in national security thinking about resilience.[41] Just as for cyber deterrence, retaliation against ambiguous or hard to detect hybrid threats may be less valuable than deterrence by denial.[42]

Another benefit is that resilience measures are vulnerability-focussed and so do not rely on predicting the form of hybrid attack. For all these reasons, resilience should form the foundation of any strategy to deter hybrid threats. For example, a recent case study of the Dutch reaction to the shooting down of flight MH17 suggests that societal resilience – in this case measured by the presence of trust, social capital, and credible narratives – has reinforced deterrence.[43]

Foundations: capability, credibility. Bolstering resilience enhances the capability available to deter hybrid threats and the credibility of doing so. While resilience measures indicate resolve, they do not communicate directly.

4.1.2. Resilience is not a strategy in itself

Yet resilience is not a strategy in itself. In one sense, resilience is *anti-strategic* – it is focussed passively inwards (on the ability to recover from shocks) rather than actively outwards on influencing others and shaping the environment. As Michael Ruhle of NATO puts it, "hoping that one could signal to an opponent 'that there's no point trying to disrupt our lives' puts a level of faith in deterrence that this concept can never live up to".[44] Moreover, deterrence by denial only works against risk-averse adversaries.[45]

Resilience also has its limits. One is the difficulty of covering every possible attack vector. The literature emphasizes protecting the political and information spheres of society, yet these are porous domains which are less amenable to government regulation than others (e.g. physical infrastructure).[46] As two Danish analysts put it, "the facts on the ground currently make resilience a challenging if not a Sisyphean task".[47]

The desirability of large-scale resilience-building is also questionable. Paradoxically, overdoing resilience and government-led intervention within the liberal-democratic model

[40] One example is the UK's 2021 Integrated Review of Security and Defence, which mentions 'resilience' 84 times and 'resilient' 28 times. See: Cabinet Office, 'Global Britain in a competitive age'.

[41] See for example: Accenture, 'The Nature of Effective Defense: Shifting from Cybersecurity to Cyber Resilience', 2018, https://www.accenture.com/_acnmedia/accenture/conversion-assets/dotcom/documents/local/en/accenture-shifting-from-cybersecurity-to-cyber-resilience-pov.pdf.

[42] Patrick M. Morgan, 'The State of Deterrence in International Politics Today', *Contemporary Security Policy*, Volume 33, Issue 1 (2012): 101, https://doi.org/10.1080/13523260.2012.659589.

[43] Cees van Doorn and Theo Brinkel, 'Deterrence, Resilience, and the Shooting Down of Flight MH17', in *NL ARMS Netherlands Annual Review of Military Studies 2020*, ed. Frans Osinga and Tim Sweijs (T.M.C. Asser Press: The Hague, 2020), https://doi.org/10.1007/978–94–6265–419–8.

[44] Michael Ruhle, 'Deterring hybrid threats: the need for a more rational debate', NDC Policy Brief (NATO Defence College, 2019), http://www.ndc.nato.int/news/news.php?icode=1335.

[45] King Mallory, 'New Challenges in Cross-Domain Deterrence' (RAND US, 2018), 3, https://www.rand.org/pubs/perspectives/PE259.html.

[46] Monaghan et al., 'MCDC Countering Hybrid Warfare', 81.

[47] Sørensen and Nyemann, 'Going Beyond Resilience', 3.

may undermine the fabric of society that one is trying to preserve in the first place, by heightening the sense of threat and weakening the "cornerstones of Western democracy—state restraint, pluralism, free media, and economic openness".[48]

Foundation: credibility. Understanding the limits of resilience enhances deterrence credibility.

4.2. Deterrence by punishment

4.2.1. Go beyond resilience: balance denial and punishment

While deterrence by denial through resilience forms a solid foundation for deterring hybrid threats, changing the behaviour of an adversary committed to hybrid aggression requires going beyond resilience to deter them through the credible threat of punishment.[49] In practice, deterring hybrid threats will require finding the right *balance* between denial and punishment, tailored to the context and actor in question.[50]

Foundation: capability. Going beyond resilience opens up more capability avenues for deterrence.

4.2.2. Diversify the playbook

The literature suggests a tendency to default to military and economic measures in threats of punishment.[51] But relying on such blunt instruments may undermine their credible use or lead to heavy-handedness. Serious hard power measures should be saved for the most egregious threats to retain their potency and manage escalation. Instead, "alternative offensive means should be found to diversify the 'playbook' for countering hybrid warfare".[52]

The same principle applies to finding targets for punishment measures which rely heavily on taking aim at the political vulnerabilities of hybrid aggressors.[53] Targeteers across government need to get creative in finding and exploiting new vulnerabilities that hybrid aggressors care about.[54] Recent progress on creative, tailored economic sanctions provides some

[48] Kenneth Payne, 'Artificial Intelligence: A Revolution in Strategic Affairs?', *Survival*, Volume 60, Issue 5 (2018): 20, https://doi.org/10.1080/00396338.2018.1518374; Mikael Wigell, 'Democratic Deterrence: How to Dissuade Hybrid Interference', *The Washington Quarterly*, Volume 44, Issue 1 (2021): 49–67, https://doi.org/10.1080/0163660X.2021.1893027.

[49] Sørensen and Nyemann, 'Going Beyond Resilience'; Duncan Allen, 'Managed Confrontation: UK Policy Towards Russia After the Salisbury Attack', Research Paper (Chatham House, 2018), https://www.chathamhouse.org/2018/10/managed-confrontation-uk-policy-towards-russia-after-salisbury-attack; Ruhle, 'Deterring hybrid threats'; Morris et al., 'Gaining Competitive Advantage'; Green and Schaus, 'Countering Coercion in Maritime Asia'.

[50] Monaghan et al., 'MCDC Countering Hybrid Warfare', 39 & 43.

[51] The survey of policy literature for MCDC shows that the majority of actions planned or proposed to deter by punishment relied on the military and economic instruments. As the authors suggest, "[t]his seems to highlight a shortfall in the ability of Western governments (the majority of the sources analyzed) to summon creative ways to escalate horizontally through offensive options". See: Aronsson, 'The state of current counter hybrid warfare policy' and Monaghan et al., 'MCDC Countering Hybrid Warfare', 79–82.

[52] Monaghan et al., 'MCDC Countering Hybrid Warfare', 81.

[53] Ibid., 82.

[54] As the MCDC Handbook puts it, "international law also provides for a wealth of measures to counter hybrid aggression without requiring the use of force...there is ample legal basis for creative horizontal escalation to counter hybrid warfare". Monaghan et al., 'MCDC Countering Hybrid Warfare', 57.

inspiration,[55] as does the promise of 'deterrence by disclosure'.[56] This 'turn every stone' approach should be applied to explore new vulnerabilities across a broader spectrum of action. However, much of this progress has been forged out of necessity in response to further violations and is (therefore) too little too late.

While punishment measures that require new regulation or legislation are more credible as a result, this can take time and be subject to legislative and political vagaries.[57] It would also be better here to prepare a diverse punishment playbook in advance. Doing so – and communicating this to adversaries – offers another opportunity to enhance the prospects of deterrence. The credibility of these measures relies on understanding two factors: what those being deterred care about and the limits of political will at home to enact such measures. To avoid the same problems of developing new punishment measures too late or too slowly, practitioners should develop diverse playbooks for deterring hybrid threats now.

Foundation: capability and credibility. Diversifying the playbook widens the capability aperture and – in doing so – enhances the credibility of deterrence.

4.3. Restrictive deterrence

4.3.1. Restrict, don't prevent, low-level hybrid threats

Restrictive deterrence seeks to minimize attributes such as effectiveness, frequency or severity, but not deter it outright. It is applicable to 'persistent' or less serious hybrid threats. What counts as a 'low-level' or 'persistent' threat will depend on setting thresholds concerning the type of threat (e.g. actor, domain, means) and level of threat severity (e.g. the intensity, impact and frequency).

This type of hybrid threat – such as nuisance misinformation or cyber interference – is not realistically deterrable in absolute terms due to ubiquity, low cost, deniability and low impact (at least in the short term). Instead, they should be managed, tolerated, or mitigated. A good way to start this conversation is to consider which hybrid threats can be tolerated, rather than which threats must be prevented.[58] One parallel is crime prevention, whereby "not all crimes can be deterred, and not all represent significant threats to national security".[59]

Rather than close down deterrence options, this approach may in fact open them up. According to MCDC:

[55] Daniel Fried and Adrian Karatnycky, 'A New Sanctions Strategy to Contain Putin's Russia', *Foreign Policy*, 4 May 2021, https://foreignpolicy.com/2021/05/04/sanctions-contain-russia-putin-west-us-eu-uk-europe-weaken-economy/; UK HMG, 'First UK Annual Sanctions Report shows how UK independent sanctions underpin Global Britain's role on the world stage', Press release, 13 January 2022, https://www.gov.uk/government/news/first-uk-annual-sanctions-report-shows-how-uk-independent-sanctions-underpin-global-britains-role-on-the-world-stage.

[56] Eric Edelman, 'The Pros and Cons of "Deterrence by Disclosure"', *The Dispatch, 21 February 2022*, https://thedispatch.com/p/the-pros-and-cons-of-deterrence-by?utm_source=url.

[57] See for example the 2017 Countering America's Adversaries through Sanctions Act, which gave Congress the power to block the lifting of sanctions (US Government, Countering America's Adversaries through Sanctions Act, PUBLIC LAW 115–44, 2 August 2017), https://www.congress.gov/115/plaws/publ44/PLAW-115publ44.pdf; see also UK's efforts to ensure sanctions relating to Russia are implemented effectively after the UK leaves the EU: HM Treasury, 'Financial sanctions, Russia', UK HMG, 2014–2022, https://www.gov.uk/government/publications/financial-sanctions-ukraine-sovereignty-and-territorial-integrity.

[58] Vladimir Rauta and Sean Monaghan, 'Global Britain in the grey zone: Between stagecraft and statecraft', *Contemporary Security Policy*, Volume 42, Issue 4 (2021): 484, https://doi.org/10.1080/13523260.2021.1980984.

[59] Wigell, 'Democratic Deterrence', 10.

> *"No longer is deterrence about absolutes. It is instead about finding ways to make attacks less likely or less effective... [This] insight is valuable because it vastly expands the range of deterrence strategies from those that can deter entirely to the wider set of those that might help in some way."*[60]

Foundation: capability and credibility. Focussing on restrictive deterrence for low-level hybrid threats provides a greater variety of options and enhances credibility through a measured approach.

4.4. Absolute deterrence: keep the relief valve open (in most cases)

Absolute deterrence seeks to prevent an action from occurring absolutely, rather than restricting and managing it. NATO's Article 5 guarantee against armed aggression is an obvious example. Absolute deterrence is a binary test of credibility: there can be no shades of grey. Given the 'warlike' dangers posed by hybrid threats – such as loss of territory, damage to critical infrastructure, erosion of the rules-based order, conventional and even nuclear escalation[61] – absolute deterrence is relevant at some level.

However, the nature of hybrid threats – gradual, ambiguous, and unconventional as they are – makes it difficult to link an immediate action to be deterred with a specific outcome to be avoided, or even a specific actor to be deterred. Restrictive deterrence may therefore be a more useful and reliable concept against most forms of hybrid aggression – at least all but the most obviously grievous or totemic. The difficulty lies in agreeing on such thresholds. This is difficult enough among domestic polities, and is potentially fiendish in the multinational context. Yet this is the exact challenge posed by hybrid threats – hence the calls for agreeing new collective thresholds such as the loss of life (e.g. through cyberattack).[62]

If it can be achieved, absolute deterrence comes with a health warning: if hybrid threats can be successfully deterred but revisionist actors remain motivated, what comes next?[63] One corollary of this observation is the argument to keep the grey zone 'relief valve' open to hybrid threats in all but the most severe cases.[64]

Foundation: credibility and communication. Keeping the relief valve open reinforces the credibility of (residual) deterrent threats, while absolute deterrence can communicate resolve.

4.5. Cumulative deterrence

Immediate deterrence has merit prior to a hybrid attack, but hybrid threats can confound traditional warnings and indicators of potential attacks.[65] Hybrid threats also challenge general deterrence because individual attacks are rarely

[60] MCDC Countering Hybrid Warfare Project, 'Hybrid Warfare: Understanding Deterrence', (MCDC Information Note, March 2019), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/795220/20190304-MCDC_CHW_Info_note_6.pdf.

[61] Rebecca Hersman, 'Wormhole Escalation in the New Nuclear Age', *Texas National Security Review*, Volume 3, Issue 3 (2020): 90–109, http://dx.doi.org/10.26153/tsw/10220.

[62] Braw, 'Biden's gray zone gaffe'.

[63] Monaghan, Countering Hybrid Warfare, 90.

[64] Sean Monaghan, 'Bad idea: winning the gray zone', CSIS, 17 December 2021, https://defense360.csis.org/bad-idea-winning-the-gray-zone/.

[65] On the invidious problem of indicators and warning for hybrid threats, see: Monaghan et al., 'MCDC Countering Hybrid Warfare', 25–32; and Cullen, 'Hybrid threats'.

significant enough to justify the design of an entire deterrence posture to prevent them. The 'snowball' effect of many low-level violations going unanswered over time can undermine the credibility of subsequent claims by the defender that they will act at *any* point in the future.

This is compounded by risk confusion, "when the hazards associated with action and inaction against gray zone rivals appear equally unpleasant".[66] Instead, a cumulative approach to deterring hybrid threats combines the immediate deterrence of specific threat increments with absolute red lines enforced to rule out never-ending gradualism and *faits accomplis*.

4.5.1. Combine immediate deterrence with absolute red lines

Cumulative deterrence seeks compound effects over time, shaping and restricting behaviour. The aim is to recharge deterrence credibility in the face of gradualist hybrid threats. Just as their power stems from the cumulative effect of coordinated actions, any approach to deterring hybrid threats must consider how to tip the balance through small steps.

This approach has recently been advocated in the context of deterring cyberattacks, grey zone strategies and Iranian aggression.[67] It can be seen as the 'mirror image' of hybrid threats: gradual, unpredictable and difficult to counter. It may also be a more credible approach than establishing red lines for adversaries to exploit (by falling just short of, or testing their credibility). As Mike Mazarr puts it (citing Thomas Schelling):

> *"When the act to be deterred is inherently a sequence of steps whose cumulative effect is what matters, a threat geared to the increments may be more credible than one that must be carried out either all at once or not at all when some particular point has been reached."*[68]

Yet cumulative deterrence still requires setting (in Schelling's words) "true red lines" for an overwhelming response (i.e. absolute deterrence). This is the only way to rule out endless transgressions or *faits accomplis*.[69] Red lines can benefit from ambiguity (e.g. over where or in what form the punishment will be inflicted) but the literature suggests best practice in most cases requires linking threats to specific deterrence outcomes.[70]

Foundation: credibility. Cumulative deterrence recharges deterrence credibility against hybrid threats.

[66] Freier, 'The Darker Shade of Gray'.

[67] Cumulative cyber deterrence seeks to "shape and limit [threats] by attacking the rival repeatedly in response to specific behaviours, over a long period of time, sometimes even disproportionally to its aggressive actions" (Uri Tor, '"Cumulative Deterrence" as a New Paradigm for Cyber Deterrence', *Journal of Strategic Studies*, Volume 40, Issue 1–2 (2017), 95, https://doi.org/10.1080/01402390.2015.1115975. In the context of Iran, Michael Eisenstadt argues for "the pursuit of advantage through cumulative, incremental gains rather than dramatic, decisive blows that are liable to be escalatory" (Eisenstadt, 'Operating in the Gray Zone'*).*

[68] Or in other, plainer, words: "The man who would kick a dog should be threatened with modest punishment for each step toward the dog, even though his proximity is of no interest in itself". Thomas Schelling, *The Strategy of Conflict*, (New Haven, CT: Yale University Press, 1960), 42, cited in: Mazarr, 'Mastering the Gray Zone', 135.

[69] Mazarr, 'Mastering the Gray Zone', 138.

[70] Barry Blechman and Stephen Kaplan, *Force Without War: U.S. Armed Forces as a Political Instrument* (Brookings Institution Press, 1978); Richard Haass and David Sacks, 'The Growing Danger of U.S. Ambiguity on Taiwan', *Foreign Affairs*, 13 December 2021, https://www.foreignaffairs.com/articles/china/2021–12–13/growing-danger-us-ambiguity-taiwan.

4.5.2. Tailoring deterrence to achieve a cumulative effect

A cumulative approach to deterring hybrid threats through small steps requires a tailored design approach to deterrence strategy. Five key principles for designing deterrence strategies tailored to hybrid threats have been proposed by MCDC.[71] These can be summarized as:

- Disaggregate hybrid threats into component parts, then target specific elements of the overall campaign with deterrence measures.
- Focus on marginal gains and targeting key vulnerabilities (of both the defender – through resilience – and the aggressor – through punishment).
- Target enabling assets. For example, disinformation can (to some extent) be blocked, attributed and fact-checked.
- Think 'performatively' about the best means to deter (i.e. the most credible – most efficient or viable – rather than the most threatening means).
- Adversary understanding is even more crucial for deterring hybrid threats – not least because more types are involved in delivering hybrid campaigns (e.g. proxies, hackers, business entities, militias, citizens, etc). Rather than complicate deterrence, this complex actor landscape actually presents more opportunities for small-step deterrence.

Foundation: credibility. Tailored deterrence enhances credibility through targeted deterrence measures based on enhanced understanding and marginal gains.

4.6. Extended deterrence

4.6.1. Extended deterrence enhances leverage but raises the credibility bar

Extending deterrence commitments to third parties offers enhanced leverage against hybrid threats through at least two mechanisms. The first is an increased deterrence 'surface area' through introducing new options for flexible deterrent action. For example, US reassurance missions in Europe offer legitimate, legal (i.e. proportionate) and scalable options to deter ambiguous hybrid aggression, short of armed conflict, which can be turned up or down.[72] They also enable further detection and deterrence options, such as surveillance or training local forces. But this is not straightforward. While heavier forces may increase the deterrent effect, they are also more difficult to justify and provide fodder for victim narratives.[73]

The second is the complication of adversary decision-making through multiplying triggers for and dimensions of deterrent action. Strengthened commitment and assurances to allies signals resolve and increases partner confidence and will to act.[74] 'Known-unknowns', such as the extended deterrence status of NATO

[71] Taken from: Monaghan et al., 'MCDC Countering Hybrid Warfare', 44–45; and MCDC, 'Hybrid Warfare: Understanding Deterrence'.

[72] The White House, 'FACT SHEET: European Reassurance Initiative and Other U.S. Efforts in Support of NATO Allies and Partners', 2014, https://obamawhitehouse.archives.gov/the-press-office/2014/06/03/fact-sheet-european-reassurance-initiative-and-other-us-efforts-support-.

[73] Bryan Frederick et al., 'Understanding the Deterrent Impact of U.S. Overseas Forces' (RAND US, 2020), https://www.rand.org/pubs/research_reports/RR2533.html.

[74] Do Young Lee, 'Strategies of Extended Deterrence: How States Provide the Security Umbrella', *Security Studies, Volume 30, Issue 5 (2021): 761–796,* https://doi.org/10.1080/09636412.2021.2010887.

non-members Finland and Sweden, or the US's strategic ambiguity on Taiwan, inject further uncertainty into the mind of the aggressor.[75] The tripwire effect of extended deterrence measures enhances guarantor credibility through 'skin in the game'.[76]

However, the benefits of extended deterrence come at a high price for credibility and can provide the adversary with more links in the deterrence chain to exploit. These principles – benefits and costs – also apply to the extension of deterrence to different forms of aggression, such as NATO's extension of Article 5 to cyber and hybrid attacks.[77] Having multiple extended deterrence commitments also tests credibility. For example, the US faces trade-offs between the security guarantees it offer to its alliance network in Europe and Asia.[78]

Foundation: capability, communication. Extended deterrence communicates resolve and introduces new dimensions of deterrent action.

4.6.2. The hyper-extension of deterrence into public and private spheres

The nature of hybrid threats necessitates the extension of security and deterrence guarantees into non-traditional – or post-modern – spheres of national security.[79] This will require tailored government protection guarantees to non-government actors.

Examples already abound. In the UK this includes the cyber and space sectors, on which government services are reliant.[80] National reserve forces are a key part of this effort. [81] In Finland, local government is helping public services and businesses to address hybrid threats.[82]

[75] Jeffrey Mankoff, 'The U.S. Faces Hard Choices on Strategic Ambiguity in Europe and Asia', *World Politics Review*, 10 December 2021, https://www.worldpoliticsreview.com/articles/30178/the-u-s-faces-hard-choices-on-strategic-ambiguity.

[76] Brian Blankenship and Erik Lin-Greenberg, 'Trivial Tripwires?: Military Capabilities and Alliance Reassurance', *Security Studies* (Feb 2022), https://doi.org/10.1080/09636412.2022.2038662.

[77] In 2014, NATO formally stated that a cyberattack could be treated by the Alliance as an armed attack (thus invoking Article 5), before doing the same for 'hybrid warfare' in 2016. The effect of this extended deterrence is difficult to judge. Although given that Article 5 has only been declared once in NATO's history, it seems unlikely that ambiguous hybrid threats might cause the next instance. See: NATO, 'Brussels Summit communiqué', 14 June 2021, https://www.nato.int/cps/en/natohq/news_185000.htm.

[78] Not least the one between its reputation for general deterrence and its prioritisation of immediate deterrence capability. See: Tongfi Kim and Luis Simón, 'A Reputation versus Prioritization Trade-Off: Unpacking Allied Perceptions of US Extended Deterrence in Distant Regions', *Security Studies*, Volume 30, Issue 5 (2021): 725–760, https://doi.org/10.1080/09636412.2021.2010889.

[79] Hence the UK Integrated Review suggests "responding to state threats can no longer be viewed as a narrow 'national security' or 'defence' agenda'" (Cabinet Office, 'Global Britain in a competitive age', 70).

[80] For example, the UK's National Cyber Security Centre (NCSC) offers expertise and resources to the private sector and the general public to combat cyberattacks: a form of deterrence by denial through enhanced resilience.

[81] Modern reservists may also be a "deterrent against overt military incursions...a defence against hybrid warfare tactics such as cyber-attacks and disinformation campaigns...[and] step in to alleviate disruptions in critical services and supplies" – but these benefits depend on governments "convincing the corporate world to rally behind them". See: Gerhard Wheeler, 'Reservists are Key to Deterrence in Grey Zone Conflict – Businesses Must Be Part of the Effort', RUSI Commentary, 30 Jan 2020.

[82] See Helsinki Region Chamber of Commerce, 'Business Community and Hybrid Threats', June 2018, http://view.24mags.com/mobilev/bbc43250c51aa3c0b599cb18066f3c2b#/page=1; The City of Helsinki, 'Helsinki in the era of hybrid threats – Hybrid influencing and the city', City of Helsinki, 2018, https://www.hel.fi/static/kanslia/Julkaisut/2018/hybridiraportti_eng_020818_netti.pdf.

In Sweden, the whole of society has been asked to contribute to national 'total defence' efforts.[83]

The question of to whom governments may consider extending deterrence against hybrid threats, and under what circumstances, are now key issues for any hybrid threat deterrence strategy. Indeed, deterrence may "no longer be primarily the concern of the armed forces but a product of deep cooperation between the military and civil society".[84]

Foundation: capability. Hyper-extending deterrence into public and private spheres multiplies the capabilities available to deter.

4.7. Reassurance

Any threat of coercion (whether deterring actions or compelling changes in existing behaviour) will be less credible without assurances to remove the threat under compliance. As Thomas Schelling put it:

> *"To say, 'One more step and I shoot', can be a deterrent threat only if accompanied by the implicit assurance, 'And if you stop I won't'".*[85]

The same idea also applies to allies and partners in the context of extended deterrence. Measures to reassure them that deterrent threats will be followed through on their behalf enhance deterrence credibility. That reassurance is a product of both resolve and capability provides flexibility in designing reassurance strategies, which could be either high resolve/low capability (e.g. 'tripwire' forces or individual sanctions) or low resolve/high capability (e.g. offshore forces or cyber defences) to achieve similar effects.[86]

Against hybrid threats, reassurance is a tool in its own right (rather than an enabler) because it can achieve useful influence effects . Reassurance is not performative, but a necessary component of extended deterrence. The range of actors that need to feel 'reassured' against the vast range of hybrid threats is much larger, from local government, to the private sector and even individual citizens.

Foundation: credibility, communication. Assurance (and reassurance) bolsters credibility by demonstrating off-ramps to aggressors and communicates seriousness.

4.8. Inducement

4.8.1. Balancing sticks with carrots

Where deterrence targets the fear of negative consequences to manipulate the decision calculus, inducement seeks to attract compliance through positive incentives. In the words of Alexander L. George:

[83] Bjorn von Sydow, 'Resilience: Planning for Sweden's "Total Defence"', *NATO Review, 4 April 2018*, https://www.nato.int/docu/review/articles/2018/04/04/resilience-planning-for-swedens-total-defence/index.html.

[84] Wheeler, 'Reservists are Key'.

[85] Schelling, *Arms and Influence*, 74. See also: Stephen Pifer, 'Managing US sanctions toward Russia', Brookings, 11 December 2020, https://www.brookings.edu/blog/order-from-chaos/2020/12/11/managing-us-sanctions-toward-russia/: "If the Kremlin concludes that the sanction will remain in place regardless of what it does, it will have no incentive to change its behavior".

[86] Blankenship and Lin-Greenberg, 'Trivial Tripwires?'.

Figure 7: A ‘suasion’ matrix showing negative and positive forms of influence.

		SUASION	
		Per-suasion **(“Do this!”)**	**Dis-suasion** **(“Don’t do that!”)**
INCENTIVES	**Positive** **(‘carrots’)**	Offer incentives and assurances	Offer alternatives
	Negative **(‘sticks’)**	Withdraw incentives and assurances	Offer disincentives

> *“What the threatened ‘stick’ cannot achieve by itself, unless it is formidable, can possibly be achieved by combining it with a ‘carrot’”.*[87]

In this sense, it is part of the same process and should be treated as such.[88] See Figure 7 for an example of this approach.[89]

Several recent authors argue for re-establishing holistic approaches to compliance-seeking strategies.[90] While the likes of George and Schelling were “acutely aware of the need to put deterrence within such broader effort space”, in recent years the carrot seems to have lost ground to the stick.[91] While the role of inducement in deterring hybrid threats is recognized by some,[92] their conclusion that inducement “may deserve more attention than it currently receives” applies here too.[93]

One way to exploit this is to accommodate limited short-term goals in exchange for longer-term stability: the ‘relief valve’ argument.[94] Such incentives also go with the grain of hybrid threats by using “a measured revisionist’s willingness to work gradually to side-step risks of conflict in the short term, while granting some of their goals”.[95] Inducement-thinking would benefit from the same creativity as punishment-thinking, and new approaches to compliance design that learn from related fields such as communication and advertising.[96] Indeed, the range of incentives on offer may be greater

[87] Alexander L. George and William E. Simons, *The Limits of Coercive Diplomacy* (Second Edition: Westview Press, 1994), 17. See also Peter Viggo Jakobsen’s idea of the ‘ideal policy’ in: Peter Viggo Jakobsen, ‘Constructing a Theoretical Framework’, Chapter 3 in *Western Use of Coercive Diplomacy after the Cold War*, ed. Peter Viggo Jakobsen (Palgrave Macmillan: London, 1998).

[88] Assurance may also be viewed as a form of positive inducement. However, the theory and practice of offering positive rewards for good behaviour is distinct from that of reassuring that threatened costs will not be imposed.

[89] Based on: Tim Sweijs et al., ‘Reimagining Deterrence: Towards Strategic (Dis)Suasion Design’, (The Hague Centre for Strategic Studies, 10 March 2020), 9, https://hcss.nl/report/reimagining-deterrence-towards-strategic-dis-suasion-design/.

[90] Paul K. Davis, ‘Toward Theory for Dissuasion (or Deterrence) by Denial’, Working Paper (RAND, 2014), https://www.rand.org/pubs/working_papers/WR1027.html; Sweijs et al., ‘Reimagining deterrence’.

[91] Sweijs et al., ‘Reimagining deterrence’, 10.

[92] See for example: Monaghan et al., ‘MCDC Countering Hybrid Warfare’; Mazarr, ‘Mastering the Gray Zone’.

[93] Sweijs et al., ‘Reimagining deterrence’, 3.

[94] Of course accommodation comes with its own risks. As MCDC put it: “[w]hile the risk of coercion is inadvertent vertical escalation, the risk of inducement is the perception of leniency – which could produce the same result”. See: Monaghan et al., ‘MCDC Countering Hybrid Warfare’, 54.

[95] Mazarr, ‘Mastering the Gray Zone’, 131.

[96] Tim Sweijs et al., ‘Reimagining Deterrence’.

as "the 'carrot' in such a strategy can be any of a variety of things the adversary values".[97] Ultimately, as with all aspects of deterrence, inducement design relies on establishing a sophisticated understanding of what the adversary wants.

Foundation: capability, credibility, communication. Inducement introduces new measures (e.g. the 'carrots'), bolsters credibility by demonstrating off-ramps to aggressors, and communicates seriousness.

4.9. Cyber deterrence: applying recent lessons to fast-forward hybrid deterrence

The challenge of deterring cyber aggression provides insights for deterring hybrid threats. Parallels between cyber and hybrid threats are notable. They include attribution difficulty, ambiguity, communication, proportionality and an uncertain retaliation calculus.[98] Cyberattacks are also well-suited as a tool of hybrid aggression (Hybrid CoE treats cyber as both a means and a threat domain).[99] Deterring hybrid threats may share the apparent limits of cyber deterrence.[100]

Another parallel – and limit – is the non-military nature of cyber and hybrid threats, which have an in-built 'escalation firebreak' effect where escalation is limited by the means used, rather than the severity of the effects of the attack.[101] This works both ways: while it reduces the likelihood of escalation (due to the proportionality principle), it also degrades deterrence by undermining the credibility of an overwhelming response.

4.9.1. Punishment, attribution, whole-of-society

Despite conceptual limits, cyber (and hybrid) deterrence may be easier in practice than in theory.[102] Cyberattacks do not occur in a contextual vacuum, so they can be linked (to some extent) to perpetrators.[103] In fact, practice may be leading theory on cyber deterrence.[104] Three ideas from the past two decades of US policy and practice of deterring cyberattacks may be directly applicable to deterring hybrid threats.

[97] In the words of Alexander L. George. He continues: "The magnitude and significance of the carrot can range from a seemingly trivial face-saving concession to substantial concessions and side-payments that bring about a stable settlement of the crisis". See: George and Simons, 'The Limits of Coercive Diplomacy'.

[98] For more on the parallels between deterring cyber and hybrid threats, see: Monaghan et al., 'MCDC Countering Hybrid Warfare', 38; and Richard Andres, 'Cyber Gray Space Deterrence', PRISM, Volume 7, Issue 2 (2017): 91–98.

[99] Giannopolous et al., 'The Landscape of Hybrid Threats'.

[100] Mariarose Taddeo, 'The Limits of Deterrence Theory in Cyberspace', *Philosophy & Technology*, Volume 31 (2017): 339–355, https://link.springer.com/article/10.1007%2Fs13347-017-0290-2.

[101] Sarah Kreps and Jacquelyn Schneider, 'Escalation firebreaks in the cyber, conventional, and nuclear domains: moving beyond effects-based logics', *Journal of Cybersecurity*, Volume 5, Issue 1 (2019): 1–11, https://doi.org/10.1093/cybsec/tyz007.

[102] David Blagden, 'Deterring cyber coercion: The exaggerated problem of attribution', *Survival*, Volume 62, Issue 1 (2020): 131–148, https://doi.org/10.1080/00396338.2020.1715072.

[103] In other words, "cyber deterrence remains connected to the physical and political worlds". Will Goodman, 'Cyber Deterrence: Tougher in Theory than in Practice?', *Strategic Studies Quarterly*, Volume 4, Issue 3 (2010): 102–135. This echoes MCDC's finding that "hybrid aggressors are deterrable" (Monaghan et al., 'MCDC Countering Hybrid Warfare', 41).

[104] Alex S. Wilner, 'US cyber deterrence: Practice guiding theory', *Journal of Strategic Studies*, Volume 43, Issue 2 (2019): 245–280, https://doi.org/10.1080/01402390.2018.1563779. See also: Piret Pernik, 'Hybrid CoE Paper 8: Cyber deterrence: A case study on Estonia's policies and practice', (Hybrid CoE, 12 October 2021), https://www.hybridcoe.fi/publications/hybrid-coe-paper-8-cyber-deterrence-a-case-study-on-estonias-policies-and-practice/.

First, an increased reliance on deterrence by punishment measures over time. The same 'denial bias' is apparent in early efforts to deter hybrid threats (see above). These efforts may also benefit from striking a better balance between punishment and denial measures, with punishment "being used hand-in-glove with denial…in practice, the two approaches reinforce each other".[105]

Second, using public attribution, or shaming, as a punishment in its own right. This approach holds promise,[106] but is not well understood.[107]

Third, developing a whole-of-society – rather than just a whole-of-government – deterrence posture. As the 2003 *US National Strategy to Secure Cyberspace* states: "Every American who can contribute to securing part of cyberspace is encouraged to do so".[108] An 'every citizen' approach to deterring hybrid threats along these lines may bear fruit.[109]

Foundation: capability, credibility, communication. Lessons from cyber deterrence can enhance all three foundations of deterrence against hybrid threats.

4.10. Re-inventing peace through rules and norms

The rules, norms and institutions that comprise the international order are designed to regulate state behaviour. Historian Michael Howard referred to this application of human agency and reason to encourage stable relations between nations as the invention of peace.[110] Hybrid threats demand a re-invention of prevailing peace concepts to regulate their occurrence.[111] This echoes the regulation of behaviour in cyberspace through new international agreements, organisations, laws and norms.[112] Legal scholars have also called for updated legal

[105] Wilner, 'US cyber deterrence', 26. See also: Michael Sulmeyer, 'How the U.S. Can Play Cyber-Offense: Deterrence Isn't Enough', *Foreign Affairs*, 22 March 2018, https://www.foreignaffairs.com/articles/world/2018-03-22/how-us-can-play-cyber-offense.

[106] In recent years, Russia (e.g. the Skripal poisoning), China (e.g. illegal island building and intellectual property theft) and Iran (e.g. supporting drone strikes on Saudi oil facilities) have all been called out for ambiguous aggression with the intent of harnessing international opinion against their actions. The success of these actions is harder to judge.

[107] Wilner, 'US cyber deterrence', 27.

[108] US Government, 'US National Strategy to Secure Cyberspace', February 2003, xiii (https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf).

[109] As above, while Cold War 'total defence' strategies are being renewed in some nations, the understanding and application of a 'whole-of-society' approach in the modern era remains immature. The aims of the *US National Strategy to Secure Cyberspace* to "raise cybersecurity awareness, train personnel, stimulate market forces, improve technology, identify and remediate vulnerabilities, exchange information and plan recovery operations" appear directly relevant to hybrid threats today (ibid).

[110] Michael Howard, *The Invention of Peace (Yale University Press, 2001).*

[111] John Raine, 'War or peace? Understanding the grey zone', IISS, 3 April 2019, https://www.iiss.org/blogs/analysis/2019/04/understanding-the-grey-zone. He calls for extending "existing conventions and regulations into the activities and means observed in the grey zone", aiming for the "inclusion of the grey zone in the realm of peaceful relations between states".

[112] Despite her views on the limits of deterrence in cyberspace, Taddeo believes cyber deterrence is possible if "a new domain-specific, conceptual, normative, and strategic framework" can be developed to underpin regulation of the behaviour of states in cyberspace. Mariarose Taddeo, 'Deterrence and Norms to Foster Stability in Cyberspace', *Philosophy & Technology*, Volume 31 (2018): 323–329, https://link.springer.com/article/10.1007/s13347-018-0328-0.

frameworks in the face of hybrid threats.[113] But this re-invention of peace will not be easy. It will "require sustained, multilateral effort, and the gains will be incremental".[114]

Foundation: credibility, communication. Developing new rules and norms can enhance the credibility of deterrence and communicate limits, boundaries and consequences.

4.11. Playing the long game

Whether or not the international rules-based system can be updated to better regulate hybrid aggression in the grey zone, the short-term imperative to deter hybrid threats will remain so that hybrid aggression does not go unopposed.[115] However, such measures need to be situated within a wider, longer-term competitive strategy to be more than simply spoilers or speed bumps. A pertinent example is US Cold War strategy, which was successful in large part because "the Western socioeconomic system was stronger, and long-term trends favored the West".[116] Hybrid threats are a function or symptom of wider social, political and economic conditions and trends. They should be understood and treated as such – not as a self-contained problem that requires solving on its own terms.

Framing the challenge in these terms provides a more useful basis on which to proceed. It may also lead to a more sobering diagnosis. Today's long-term trends are different from the Cold War. To some extent, they suggest that revisionists and challengers are gaining in strength and number, while the status quo powers are in relative decline. NATO's Michael Ruhle sees hybrid threats within this context, as "another manifestation of the West falling out of its illusion that it will continue to dominate the international system".[117] If true, this will require new thinking about how to compete in and win the long game.

Foundation: capability. Seeing the bigger picture and playing the long game can broaden deterrence leverage (e.g. through bringing non-traditional domains into play, such as values and technology competition).

4.12. Lessons from the '45-year-long grey zone struggle'

The Cold War has been described as a 45-year-long 'grey zone' struggle.[118] Novel approaches were developed by Western governments to deter and counter Soviet 'active measures' and other measures short of war during that period. Several insights and lessons stand out for the practice of deterrence against hybrid threats.

[113] Aurel Sari, 'Hybrid threats and the law: Building legal resilience' (Hybrid CoE Research Report 3, November 2021), https://www.hybridcoe.fi/publications/hybrid-coe-research-report-3-hybrid-threats-and-the-law-building-legal-resilience/.

[114] Raine, 'War or peace?'.

[115] See for example: Melanie W. Sissons, 'A Strategy for Competition', CNAS, 27 August 2020, https://www.cnas.org/publications/commentary/a-strategy-for-competition; Katie Crombe et al., 'Integrating deterrence across the gray — making it more than words', Military Times, 8 December 2021, https://www.militarytimes.com/opinion/commentary/2021/12/08/integrating-deterrence-across-the-gray-making-it-more-than-words/; Clementine Starling et al., 'Seizing the advantage: The next US National Defense Strategy', (Atlantic Council, December 2021), 47, https://www.atlanticcouncil.org/wp-content/uploads/2021/12/Seizing-the-Advantage_A-Vision-for-the-Next-US-National-Defense-Strategy.pdf.

[116] Mazarr, 'Mastering the Gray Zone', 119.

[117] Ruhle, Deterring Hybrid Threats, 4.

[118] Joseph L. Votel, 'Unconventional Warfare in the Gray Zone', *Joint Force Quarterly*, Volume 80, January 2016, https://ndupress.ndu.edu/JFQ/Joint-Force-Quarterly-80/Article/643108/unconventional-warfare-in-the-gray-zone/.

- Cold War concepts such as 'flexible response' and 'total defence' can be modernized against hybrid threats.[119]
- The importance of a coherent approach – or doctrine – for assertive measures (like 'containment' or 'flexible response').[120]
- Assertive measures were complemented by simpler and cheaper methods to deter by denial, such as exposing disinformation.[121]
- Organizational design was novel, adaptive and responsive to the priorities of changing administrations.[122]
- A balance between oversight and freedom of action is required.[123]
- Collaboration is key – across government, the private sector and society.[124]

The most salient insight from this analysis might be that what has worked before may work again. Moreover, through leveraging modern technology, these approaches may achieve greater effectiveness than before.[125]

Foundation: capability, credibility, communication. Applying Cold War lessons can strengthen all three pillars of deterrence.

4.13. The limits of deterrence

Deterrence, like any strategy, has limits. Aside from the fundamental and deep-rooted limits on knowing what an adversary is thinking or how they may react – hence the aphorism deterrence is an art not a science[126] – deterrence has specific conceptual limits against hybrid threats. These add up to the insight that "one

[119] Monaghan et al., 'MCDC Countering Hybrid Warfare', 44.
[120] The guiding principles of George Kennan's 'containment' strategy and the inauguration of 'political warfare' are well known (see: Office of the Historian, 'Kennan and Containment, 1947', US Dept of State, https://history.state.gov/milestones/1945–1952/kennan; George F. Kennan, 'The Inauguration of Organized Political Warfare' [Redacted Version], 30 April 1948, History and Public Policy Program Digital Archive, https://digitalarchive.wilsoncenter.org/document/114320.pdf?v=94). The associated, subsequent doctrine of 'flexible response' was "a mobile, substantial, and flexible US capability for operations short of general war to meet the threat of limited aggression", guided by principles of moderation, proportionality and the primacy of diplomacy. See: Justin Tiplady, 'How did the Doctrine of Flexible Response Contribute to the Resolution of the Berlin Crisis of 1961?' (2011), 5, https://www.jfki.fu-berlin.de/academics/SummerSchool/Dateien2011/Papers/basosi_tiplady.pdf).
[121] For example, the Reagan-era US Active Measures Working Group (AMWG) was an empowered, agile cross-government body with a modest remit. The group could expose disinformation at a fraction of the cost necessary for the Soviets to create and distribute it. One report specifically recommends re-establishing the AMWG. See: Kathleen H. Hicks et al., 'By Other Means Part II: Adapting to Compete in the Gray Zone', (CSIS, 2019) viii, https://www.csis.org/analysis/other-means-part-ii-adapting-compete-gray-zone.
[122] A 'task force' model worked well, providing inherent lines of authority and flexibility to change in a long-haul campaign. Layers and hierarchy should be minimized, organizations empowered and initiative encouraged. See: Hicks et al., 'By Other Means Part II', 69–71.
[123] The proliferation of covert and clandestine activities in response to grey zone-like threats led to many innovations and successes (such as the CIA's role in covert action). But minimizing legislative oversight of these led to myopia and inertia. Done right, oversight should enable effective policy, not impede it. See: Kath Hicks et al., 'By Other Means Part II', 70.
[124] For example, public-private collaboration on information operations "was a major element of Western solidarity". See: Kath Hicks et al., 'By Other Means Part II', 71.
[125] Steve Abrams, 'Beyond Propaganda: Soviet Active Measures in Putin's Russia', *Connections*, Volume 15, Issue 1 (2016): 27–28, http://www.jstor.org/stable/26326426.
[126] This is implied by, amongst others, Colin Gray: Colin S. Gray, 'Deterrence in the 21st century', *Comparative Strategy*, Volume 19, Issue 3 (2000): 255–261, https://doi.org/10.1080/01495930008403211.

must accept that some hybrid threats cannot be deterred",[127] because they are too numerous or low-level, because the perpetrator is too committed, because the cross-domain deterrence logic is too complex, or because deterrence has already failed.

4.13.1. Lower limits: not all hybrid threats can be deterred all the time

The lower limits of deterrence require the least serious hybrid threats to be simply tolerated or absorbed: not all hybrid threats can be deterred all the time. For hybrid threats, the lower limits of deterrence can be found where the range of possible modes of attack are too numerous to target (or simply unknown), or the costs of each individual violation are too low to justify taking measures – or taking a risk – to deter. This was the essential logic behind US Cold War strategy, which sought to focus limited resources on addressing the most consequential Soviet actions,[128] rather than to deter and react to every minor transgression. Less consequential actions were tolerated or absorbed. This approach contained the Soviet threat while allowing the larger trends – the shortcomings of the Soviet system and the relative strength of the liberal-democratic-capitalist model – to work in their favour.

Foundation: credibility. Understanding the lower limits of deterrence enhances credibility.

4.13.2. Upper limits: the deterrence gap short of armed conflict

The upper limits of deterrence suggest that even the most serious hybrid threats cannot be reliably deterred, leaving a 'deterrence gap' short of armed conflict. The upper limits of deterrence are exposed when the perpetrator is more committed or risk tolerant than the defender. If the defender is perceived as unwilling (or unable) to enforce red lines or limits on aggression, deterrence may well fail. This returns to a fundamental challenge of deterring hybrid threats: the defender's dilemma.

Assuming the defender's credibility is reset above the line of armed attack (around which conventional deterrence thresholds are set – such as NATO's Article 5), this leaves a 'deterrence gap' short of armed conflict for the perpetrator to exploit. The 'escalation firebreak' limitation mentioned above adds to this difficulty. If public support cannot be generated for an overwhelming decisive response to a non-military hybrid threat, the whole strategy of deterrence is undermined because the credibility of any threatened punishment has disappeared.

Foundation: credibility. Understanding the upper limits of deterrence enhances credibility by avoiding over-extension.

4.13.3. Escalation ladder complexity

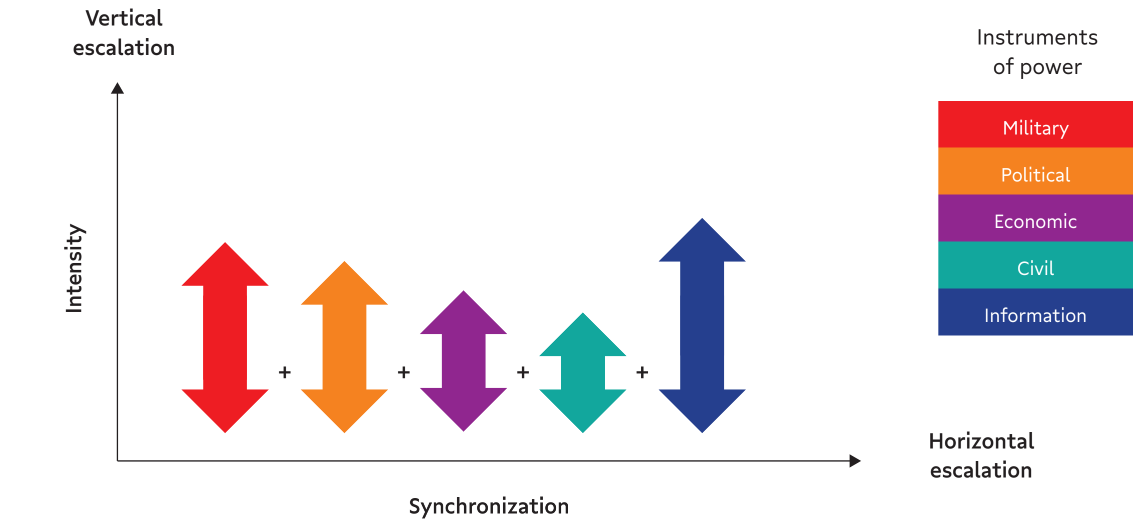
The potential variety and novelty of hybrid threats complicates the 'escalation ladder' of threats to deter.[129] This complex escalation

[127] Ruhle, 'Deterring Hybrid Threats', 4.

[128] I.e. those that might provide political momentum to the global communist movement, directly threaten US national security or trigger nuclear war.

[129] For example, MCDC use the PMESII domains of action – political, military, economic, social, information, infrastructure – and the MPECI levers of power – military, political, economic, civil, informational. See Monaghan et al., 'MCDC Countering Hybrid Warfare'. For the (original) 'escalation ladder', see Herman Kahn, *On Escalation: Metaphors and Scenarios* (New York: Frederick A. Praeger, 1965). For more on the cross-domain deterrence problem see: Dmitry Adamsky, 'Cross-Domain Coercion: The Current Russian Art of Strategy', Proliferation Papers, No. 54 (IFRI, November 2015), https://www.ifri.org/en/publications/etudes-de-lifri/proliferation-papers/cross-domain-coercion-current-russian-art-strategy; Mallory, 'New Challenges in Cross-Domain Deterrence'; Erik Gartzke and Jon R. Lindsay, *Cross-Domain Deterrence* (Oxford University Press, 2019).

Figure 8: The hybrid threat escalation ladder, with vertical and horizontal components



landscape also increases the potential for unintended escalation. As one analysis describes this challenge:

> *"[T]he strategic implications of complex linkages between actions and effects across boundaries – the potential for escalation, the interpretation of signals, even the effects of operations – are as yet still poorly understood. To compound the confusion, policymakers may not yet know how their own governments will respond to unconventional attacks."*[130.]

Figure 8 above shows the escalation landscape of hybrid threats, which can combine 'horizontal' escalation – by using different instruments of power – and 'vertical' escalation – by increasing the intensity of each one.[131.]

Foundation: capability, communication. Exploiting the complex escalation landscape can broaden the capabilities available to deter hybrid threats and provide more deterrence communication opportunities.

4.13.4. Beyond deterrence

Finally, an important limit of deterrence in countering hybrid threats is a conceptual one: if an adversary is *already engaged* in a campaign of hybrid aggression, then deterrence has failed to some extent. The only relevance that deterrence has to such a situation is in seeking to prevent more serious attacks. In reality, countering hybrid threats in any meaningful way therefore requires going beyond deterrence (see Section 5.3).

4.14. Restoring the foundations

Hybrid threats undermine the 'three Cs' of deterrence in specific ways (see Section 3.3 above). Table 2 below shows how the insights developed in this section can help restore these foundations of deterrence – brick by brick.

4.15. A framework for deterring hybrid threats

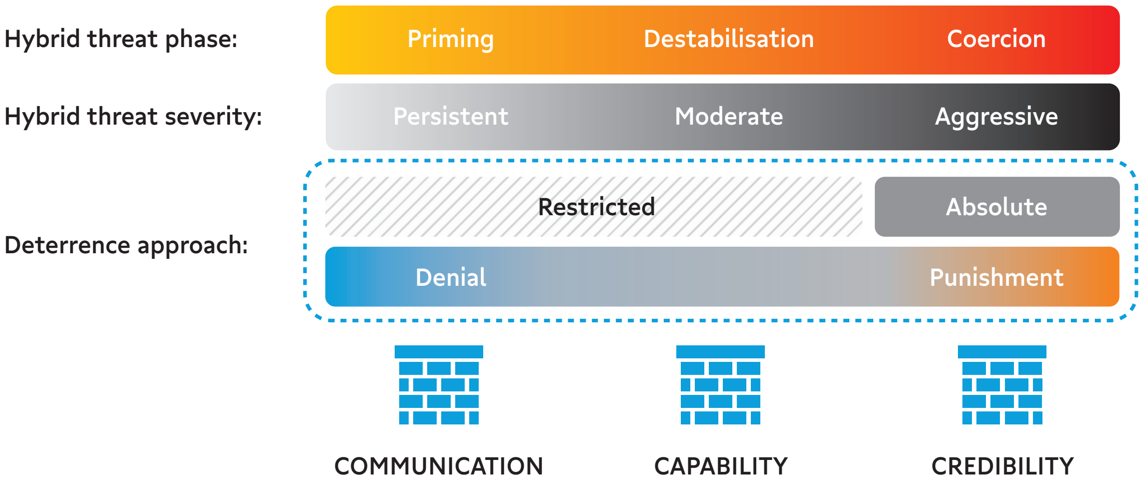
Figure 9 below integrates many of the insights and principles above into a framework for deterring hybrid threats. From top to bottom, it shows the 'phase' of hybrid activity (according to Hybrid CoE's typology), the severity of hybrid threat (based on RAND's levels), and the key components of any deterrence strategy related to the phase and severity.

[130.] Erik Gartzke and Jon Lindsay, 'Cross-Domain Deterrence: Strategy in an Era of Complexity', 15 July 2014, 3, https://quote.ucsd.edu/deterrence/files/2014/12/EGLindsay_CDDOverview_20140715.pdf.
[131.] Taken from Monaghan et al., 'MCDC Countering Hybrid Warfare', 14.

Table 2: Mapping report insights into the three pillars of deterrence

	Capability	Credibility	Communication
Resilience is the foundation of hybrid deterrence	✓	✓	
Resilience is not a strategy in itself		✓	
Go beyond resilience: balance denial and punishment	✓		
Diversify the playbook	✓	✓	
Restrict, don't prevent, low level hybrid threats	✓	✓	
Keep the relief valve open (in most cases)		✓	✓
Combine immediate deterrence with absolute red-lines		✓	
Tailor deterrence to achieve cumulative effect		✓	
Extended deterrence enhances leverage but raises the credibility bar	✓		✓
The hyper-extension of deterrence into public and private spheres	✓		
Assurance (and reassurance)		✓	✓
Balancing sticks with carrots	✓	✓	✓
Cyber: Punishment, attribution, whole-of-society	✓	✓	✓
Re-inventing peace through rules and norms		✓	✓
Playing the long game	✓		
Lessons from the '45-year long grey zone struggle'	✓	✓	✓
Lower limits: not all hybrid threats can be deterred all the time		✓	
Upper limits: the deterrence gap short of armed conflict		✓	
Escalation ladder complexity	✓		✓

Figure 9: A framework for deterring hybrid threats



5. New horizons

This final section points to four new horizons for further development and research:

- the role of military force in deterring hybrid threats;
- going beyond deterrence to counter hybrid threats;
- the future evolution of hybrid threats and implications for deterrence;
- the prospect of a post-modern, 'fifth wave' of deterrence theory and practice that is centred on deterring hybrid threats.

5.1. The role of military force in deterring hybrid threats

Conventional deterrence through military force does not play a central role in Hybrid CoE's *Deterrence Playbook*, which "goes far beyond military-centric classical deterrence thinking".[132] Yet hard power is still the *sine qua non* of deterrence.[133] The relevance to hybrid threats is, to some extent, a matter of perspective. On the one hand, hybrid threats suggest that conventional deterrence is succeeding: revisionists are not resorting to armed attacks. On the other hand, hybrid threats suggest that conventional deterrence is failing: revisionists are still exhibiting aggressive behaviour (albeit through non-violent means). Either way, it seems likely that conventional deterrence shapes the use of hybrid threats.

5.1.1. Seeing the bigger picture

One way of appreciating the role of conventional military deterrence against hybrid threats is to see the bigger picture beyond the edges of competition in the grey zone between peace and war.[134] Figure 10 below shows grey zone competition in a continuum of relations between states. It shows how changes in the intensity of relations can lead to new phases once tipping points have been reached – including boiling over from hybrid threats to armed conflict. These changes are driven by both amplifying and suppressive dynamics.

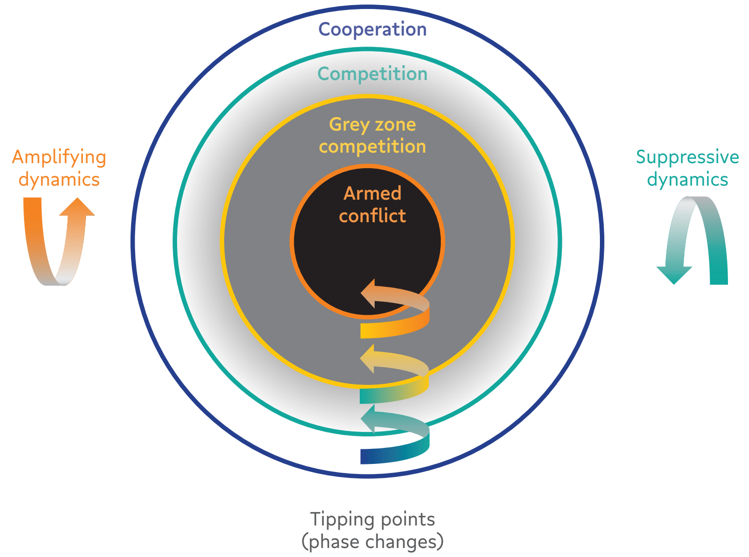
Seeing this bigger picture beyond the 'grey zone' in which hybrid threats operate helps in understanding how conventional and nuclear deterrence – in other words, escalation dominance in armed conflict – can have an important *latent* deterrent effect against hybrid threats. This effect acts to both suppress the severity of hybrid threats and to prevent them from boiling over into armed conflict. In the words of British Army Chief, General Sir Mark Carleton-Smith,

[132] Although it rightly advocates the integration of "civil and military elements" and recognizes the need to "consider a range of both military and non-military response options". Kersanskas, 'Deterrence', 8, 15. The same point is made by many others, including in a chapter on deterrence in East Asia, titled 'Beyond Military Deterrence'. See: Chin-Hao Huang and David C. Kang, 'Beyond Military Deterrence: The Multidimensionality of International Relations in East Asia', Chapter 14 in *Cross-Domain Deterrence*, ed. Erik Gartzke and Jon Lindsay (Oxford University Press, 2019), https://oxford.universitypressscholarship.com/view/10.1093/oso/9780190908645.001.0001/oso-9780190908645-chapter-14. See also James Lewis, who states: "Deterrence based on military force is still valuable for dissuading opponents from undertaking certain kinds of attack, but this may need to be buttressed by political actions that go beyond classic, force-based deterrence" (Lewis, 'Cross-Domain Deterrence and Credible Threats').

[133] As one author notes: "Looking forward, there appears to be little reason to expect conventional deterrence to wane in importance relative to other elements of national security policy in the near future." Karl Mueller, 'The Continuing Relevance of Conventional Deterrence', Chapter 4 in *Annual Review*, ed. Sweijs and Osinga (T.M.C. Asser Press: The Hague, 2020), 60. See also: Robert P. Haffa Jr, 'The Future of Conventional Deterrence: Strategies for Great Power Competition', *Strategic Studies Quarterly*, Volume 12, Issue 4 (2018): 94–115.

[134] Monaghan, 'Bad idea: winning the gray zone'.

Figure 10: Grey zone competition (where hybrid threats operate) in a continuum of relations between states[135]



"competitors operate below the threshold of war precisely because we maintain one".[136] Or as former NATO Supreme Allied Commander Europe, General Philip M. Breedlove, puts it, "the best defence against 'little green men' is 'big green men'".[137]

5.1.2. Three dimensions: relevance, utility and trade-offs

Using military force short of war to deter is a long-established practice. The history of military force is more often about peace than war.[138] Hybrid CoE's *Playbook* highlights contemporary examples, observing that "port visits, snap exercises, the use of defence attaché networks, and other activities can be part of a coordinated response and can even be decisive in changing the cost-benefit calculus of the hostile actor".[139] However, relying on the use of force short of war invites a trade-off problem vis-à-vis its role in conventional deterrence (i.e. the ability to prosecute high-end warfighting).[140]

[135] Adapted from an internal report by the UK's Defence Science and Technology Laboratory. With thanks to Dr Gordon Niven.

[136] UK Ministry of Defence, 'The Chief of the General Staff: Tomorrow's army – An asymmetric army for the digital age', The British Army, 8 October 2020, https://www.army.mod.uk/news-and-events/news/2020/10/cgs-tomorrow-s-army/. See also Jack Watling, who says: "the ability to escalate to a point unacceptable to an adversary, and the threshold at which that escalation will occur, sets the parameters for 'grey zone' activity... The balance of deterrence fixes the confrontation within understood limits" (Jack Watling, 'We Need to Relearn How to do Deterrence', RUSI Commentary, 5 December 2019, https://rusi.org/explore-our-research/publications/commentary/we-need-relearn-how-do-deterrence).

[137] Quoted in Ruhle, 'Deterring hybrid threats', 2. See also: Geoff Hertenstein, 'DIME without the 'M' is DIE', *The Strategy Bridge*, 22 Sept 2019, https://thestrategybridge.org/the-bridge/2019/9/22/dime-without-the-m-is-die-a-case-for-conventional-military-power-in-modern-strategy-discourse.

[138] For studies of this see for example: Blechman et al., *Force Without War*; Barry M. Blechman et al., *Military Coercion and US Foreign Policy: The Use of Force Short of War* (Routledge, 2020); Rupert Smith, *The Utility of Force: The Art of War in the Modern World* (London: Penguin, 2005).

[139] Kersanskas, 'Deterrence', 15.

[140] Hal Brands, 'Pentagon's new plan to fight China and Russia in the gray zone', *Bloomberg Opinion*, 21 October 2021, https://www.aei.org/op-eds/pentagons-new-plan-to-fight-china-and-russia-in-the-gray-zone/; Monaghan, 'Countering Hybrid Warfare', 91–92; Monaghan, 'Bad idea: winning the gray zone'; Becca Wasser et al., 'Risky Business: Future Strategy and Force Options for the Defense Department', CNAS, July 2021, https://www.cnas.org/publications/reports/risky-business-future-strategy-and-force-options-for-the-defense-department.

When it comes to hybrid threats or 'hybrid war', a pertinent question is: Are we most worried about the 'hybrid' or the 'war'?[141]

The role of military force in deterring hybrid threats is at the heart of current debates over defence strategy in many nations. To adapt to "a competitive age",[142] defence forces will be required to "walk a tricky line: preparing for war with other great powers while making peacetime efforts to ensure that war never happens".[143]

Notably, the US Department of Defense has placed the concept of 'integrated deterrence' at the core of its contribution to the 'strategic competition' with China and others.[144] The same question will be at the heart of the debate over NATO's new Strategic Concept given that it recognizes that "strategic competition is rising".[145] With Russia's armed aggression against Ukraine and designs on Europe's security order, NATO must articulate a new approach to deterrence and defence against both conventional war and hybrid threats. Hence NATO's two new 'capstone concepts': one for warfighting, and one for deterrence.[146]

This brief discussion puts forward three key ideas about the role of conventional deterrence against hybrid threats: it is relevant; there is widespread utility; and there is likely to be a trade-off between utility short of war and high-end warfighting. Yet despite its relevance and importance, the role of military force in deterring hybrid threats is under-conceptualized.[147] Further research is required to go beyond these general principles. A small number of studies have begun this task and are worth pointing to.

Relevance

In terms of the first dimension (the relevance of conventional military deterrence to hybrid threats), war games by RAND US suggest that the main effect is to "deter high-order aggression" rather than hybrid "grey zone tactics",

[141] The answer should be obvious. In Andrew Monaghan's pithy formulation regarding Russian 'hybrid warfare', watch out for "The 'War' in Russia's 'Hybrid Warfare'". Andrew Monaghan, 'The "War" in Russia's "Hybrid Warfare"', *Parameters*, Volume 45, Issue 4 (2015), https://press.armywarcollege.edu/parameters/vol45/iss4/8.

[142] To use the title from the UK's recent defence and security review: Cabinet Office, 'Global Britain in a competitive age'.

[143] Brands, 'Pentagon's new plan'.

[144] The White House, 'Interim National Security Strategic Guidance', March 2021, https://www.whitehouse.gov/wp-content/uploads/2021/03/NSC-1v2.pdf; Jim Garamone, 'Concept of Integrated Deterrence Will Be Key to National Defense Strategy, DOD Official Says', DOD News, 8 December 2021, https://www.defense.gov/News/News-Stories/Article/Article/2866963/concept-of-integrated-deterrence-will-be-key-to-national-defense-strategy-dod-o/. It is worth noting that the term 'integrated deterrence' remains ill-defined. For one illuminating attempt at clarity, see: Frank Hoffman, 'Conceptualizing Integrated Deterrence', Lawfire, 8 January 2022, https://sites.duke.edu/lawfire/2022/01/08/guest-post-dr-frank-hoffman-on-conceptualizing-integrated-deterrence/.

[145] NATO, 'NATO 2022 Strategic Concept', NATO HQ, https://www.nato.int/strategic-concept/.

[146] NATO ACT, 'NATO Chiefs of Defence Focus on the Alliance's Military Instrument of Power', 14 January 2022, https://www.act.nato.int/articles/nato-mccs-2022–1.

[147] For example, see debates over the forthcoming US National Defence Strategy, which will be founded on the concept of 'integrated deterrence': Thomas Spoehr, 'Bad Idea: Relying on "Integrated Deterrence" Instead of Building Sufficient U.S. Military Power', Defense 360°, 3 December 2021, https://defense360.csis.org/bad-idea-relying-on-integrated-deterrence-instead-of-building-sufficient-u-s-military-power/; Becca Wasser and Stacie Pettyjohn, 'Why the Pentagon Should Abandon "Strategic Competition"', *Foreign Policy*, 19 October 2021, https://foreignpolicy.com/2021/10/19/2022-us-nds-national-defense-strategy-strategic-competition/.

which are best countered by "civil organizations".[148] Another RAND study – based on case studies and historical analysis – offers a different view: a military presence and posture short of war can deter the most serious hybrid threats through signalling and reinforcing partners.[149] In fact, in cases of extended deterrence, "the ability of local U.S. forces to win a contest outright is of less importance than the presence of some forces".[150] These competing claims deserve further investigation through dedicated inquiry via a diversity of methods – including empirical and operational research using recent case studies.

Utility

One example is a recent study on US military coercion short of war,[151] which examines the second dimension of the breadth of the utility of military force in deterrence short of war. The authors draw three broad conclusions. First, the military has broad utility to achieve coercive effects (such as deterrence) short of war, from capacity and resilience-building to demonstrations of force. Second, coercion short of war is difficult. In the cases studied, the success rate was about 50% – and these cases mostly achieved short-term effects (less than six months) such as buying time for diplomacy. That said, deterrence is easier than compellence, which requires changing existing behaviour.[152] Third, factors associated with success include demonstrating a consistent pattern of commitment, moving forces from 'outside to in' the theatre of concern, understanding an adversary's perceptions and linking clear, specific demands to coercive threats (ambiguity is generally not helpful).

Trade-offs

In terms of the third dimension of trade-offs, plenty of authors identify the need to examine the relationship between maintaining the credibility of conventional high-end military deterrence, and dedicating more resources to countering hybrid threats through the prism of 'daily competition'.[153] However, there are fewer studies that take on this analytical challenge.

[148] Pettyjohn and Wasser, 'Competing in the Gray Zone'.

[149] Michael J. Mazarr et al., 'What Deters and Why: Exploring Requirements for Effective Deterrence of Interstate Aggression', Research Report (RAND, 2018), https://www.rand.org/pubs/research_reports/RR2451.html.

[150] Mazarr et al., 'What Deters and Why: Exploring Requirements for Effective Deterrence of Interstate Aggression', 15.

[151] Blechman et al., *US Military Coercion*. See also the original study: Blechman et al., Force Without War.

[152] The authors (Blechman et al., *Force Without War*) refer to this as 'reinforcing' behaviour (through deterrence, reassurance etc.) vs. 'modifying' behaviour (through compellence, inducement etc.). As Thomas Schelling says: "it is easier to deter than compel" (Schelling, *Arms and Influence* (2020 Edn), 100). The claims made by Prospect Theory also help explain this observation. See: Daniel Kahneman and Amos Tversky, 'Prospect Theory: An Analysis of Decision under Risk', *Econometrica*, Volume 47, Issue 2 (1979): 263–291, https://doi.org/10.2307/1914185; and Robert Jervis, 'Political Implications of Loss Aversion', *Political Psychology*, Volume 13, Issue 2 (1992): 187–204, https://doi.org/10.2307/3791678.

[153] See for example: Monaghan, 'Countering Hybrid Warfare: So What for the Joint Force?'; Monaghan et al., 'MCDC Countering Hybrid Warfare'; Mazarr et al., 'What Deters and Why'; Morris et al., 'Gaining Competitive Advantage'; Green and Schaus, 'Countering Coercion in Maritime Asia'; Brands, 'Pentagon's new plan'; Watling, 'We Need to Relearn How to do Deterrence'; Kathleen H. Hicks et al., 'By Other Means Part I: Campaigning in the Gray Zone', Report (CSIS, 2019), https://www.csis.org/analysis/other-means-part-i-campaigning-gray-zone; Jim Mitre and Andre Gellerman, 'Defining DoD's Role in Gray Zone Competition', CNAS, 24 August 2020, https://www.cnas.org/publications/commentary/defining-dods-role-in-gray-zone-competition; Stacie L. Pettyjohn and Becca Wasser, 'Don't Sweat the Small Stuff: Getting Force Design Right in the Next National Defence Strategy', War on the Rocks, 12 October 2021, https://warontherocks.com/2021/10/dont-sweat-the-small-stuff-getting-force-design-right-in-the-next-national-defense-strategy/.

One notable recent example is a study by the US think-tank the Center for a New American Security (CNAS).[154] It uses judgement-based tabletop exercises to examine the question: "Is the Pentagon's priority to compete below the threshold of armed conflict, or is it to prepare to defeat a great-power adversary in a large-scale war to strengthen deterrence?". The authors compare a military strategy focussed on 'high-end deterrence' with one focussed on 'daily competition' (against hybrid threats) and conclude that "the high-end deterrence strategy is the best path forward".[155] Even a military strategy optimized for deterring hybrid threats short of conventional deterrence is unlikely to succeed, according to the authors – not to mention the "significant escalatory risks" of such an approach.[156]

Another noteworthy – but narrower – analysis concerns how (and whether) deterrence works against 'sub-conventional' violations of Estonian airspace by Russia.[157] It uses insights from criminology studies to assess NATO's deterrence as "elusive, because there is no consistency in responding to these violations and no meaningful punishment".[158] It sees a clear role for military assets to enhance deterrence through both air policing responses to incursions and increased intelligence, surveillance and reconnaissance (ISR) flights, both of which would impose costs. This finding is partly based on insights from the "criminological literature [which] unambiguously shows that the severity of the punishment is less important than the certainty and swiftness of the sanctions".[159]

5.1.3. Further research: precedents and promising avenues

The important implications of the role of conventional military deterrence against hybrid threats combined with the paucity of detailed studies on this question suggests that more research is required. Such analysis has both precedents and promising avenues. One precedent is the challenge of balancing forces between "long-term stability operations or high-intensity conflict".[160] Rather than demand such a false dichotomous choice, Frank G. Hoffman advocated multi-modal hybrid threats as "a better focal point for considering alternative joint force postures".[161] The same approach may be relevant in considering the role of military force against today's hybrid threats.

[154] Wasser et al., 'Risky Business'.
[155] Ibid., 1.
[156] In their words: "The competition strategy bets that a large and visible force that actively contests daily military provocations will deter both sub-conventional and conventional aggression, even if the force is not capable of stopping either type of attack… We conclude that it is unlikely that competition can be won by the military, even one optimized to face this challenge". See Wasser et al., 'Risky Business', 26.
[157] Matus Halas, 'NATO's sub-conventional deterrence: The case of Russian violations of the Estonian airspace', *Contemporary Security Policy* (2022): https://doi.org/10.1080/13523260.2022.2028464.
[158] Halas, 'NATO's sub-conventional deterrence', 1.
[159] Ibid., 21.
[160] Frank G. Hoffman, 'Hybrid Threats: Reconceptualizing the Evolving Character of Modern Conflict', *Strategic Forum*, Issue 240 (April 2009): 1, https://www.files.ethz.ch/isn/98862/SF240.pdf.
[161] Hoffman, 'Hybrid Threats'.

With this in mind, promising avenues for analyzing trade-off problems include those used in multi-objective or 'robust' decision-making.[162] These techniques have been employed to analyze military force design portfolios in US 'security cooperation' missions.[163] There is also a range of tools available to consider a high-level force design portfolio and strategic choices to support this analysis.[164]

Finally, it is worth noting that many nations have already drawn initial conclusions to the question of conventional military deterrence relevance and codified the answers in their national defence strategies. Prominent recent examples include the UK, Australia, and the US Marine Corps – all of which come to seemingly different conclusions and investment priorities about the role of military force in deterring hybrid threats.[165] For all of these reasons, more research and analysis is required on this question – as a matter of priority.[166]

5.1.4. Nuclear deterrence

A brief word on nuclear deterrence is also required. At first glance, the destructive power of nuclear weapons makes them irrelevant to low-level hybrid aggression. But nuclear weapons have played a role in the emergence and implementation of hybrid threats. Nuclear weapons provide a powerful mutual incentive to relegate competition and conflict to the grey zone, where the risks of nuclear escalation are lower.[167] This 'stability-instability paradox' results from the relative stability of nuclear deterrence driving instability down to lower levels.[168]

Nuclear weapons may also be employed within campaigns of hybrid aggression.[169] A nuclear 'perimeter' around a hybrid campaign

[162] Robert J. Lempert et al., 'Shaping the Next One Hundred Years: New Methods for Quantitative, Long-Term Policy Analysis', Monograph Report (RAND, 2003), https://www.rand.org/pubs/monograph_reports/MR1626.html; Robert J. Lempert, 'Robust Decision Making (RDM)', in *Decision Making under Deep Uncertainty: From Theory to Practice*, ed. Vincent Marchau et al. (Springer, Cham, 2019) (Open Access: https://link.springer.com/book/10.1007/978–3–030–05252–2); Yakov Ben Haim, 'Dealing with Uncertainty in Strategic Decision-making', *Parameters*, Volume 45, Issue 3 (2015): 63–73, https://press.armywarcollege.edu/cgi/viewcontent.cgi?article=2743&context=parameters.

[163] Stephen W. Popper, 'Robust decision making and scenario discovery in the absence of formal models', *Futures and Foresight Science*, Volume 1, Issue 3–4 (Sept–Dec 2019): https://doi.org/10.1002/ffo2.22.

[164] See for example: Thomas G. Mahnken et al., 'America's Strategic Choices: Defense Spending in a Post-COVID-19 World', Report (Centre for Strategic and Budgetary Assessments, 14 January 2021), https://csbaonline.org/research/publications/americas-strategic-choices-defense-spending-in-a-post-covid-19-world; CSIS, AEI and War on the Rocks, 'The Defense Futures Simulator', https://www.defensefutures.net/; Michael E. Linick, 'Hedgemony: A Game of Strategic Choices', Wargame (RAND, 2020), https://doi.org/10.7249/TL301.

[165] For a discussion of this, see: Monaghan and Rauta, 'Global Britain in the grey zone', 476 and 486.

[166] This call is also made regarding the role of defence in countering hybrid threats writ large in: Monaghan and Rauta, 'Global Britain in the grey zone', 485–486.

[167] See for example: Michael J. Mazarr, 'Struggle in the Gray Zone and World Order', *War on the Rocks*, 22 December 2015, https://warontherocks.com/2015/12/struggle-in-the-gray-zone-and-world-order/; Hal Brands, 'Paradoxes of the Gray Zone', FPRI, 5 February 2016, https://www.fpri.org/article/2016/02/paradoxes-gray-zone/; Mazarr et al., 'Understanding the Emerging Era of International Competition', 25, 30.

[168] Originally proposed in Snyder, *Deterrence and Defense*. See also: Richard Ned Lebow, *Between Peace and War* (Johns Hopkins University Press, 1981).

[169] Mazarr, 'Mastering the Gray Zone', 61.

can condition the response of the target(s).[170] For example, nuclear coercion – through rhetoric, signalling and posturing – may have enhanced Russia's freedom of action to invade Ukraine in 2014 and 2022 by deterring outside intervention.[171] As for conventional military power, it may be more accurate to describe the role of nuclear weapons as an enabler of hybrid threats, rather than a specific lever of power.[172]

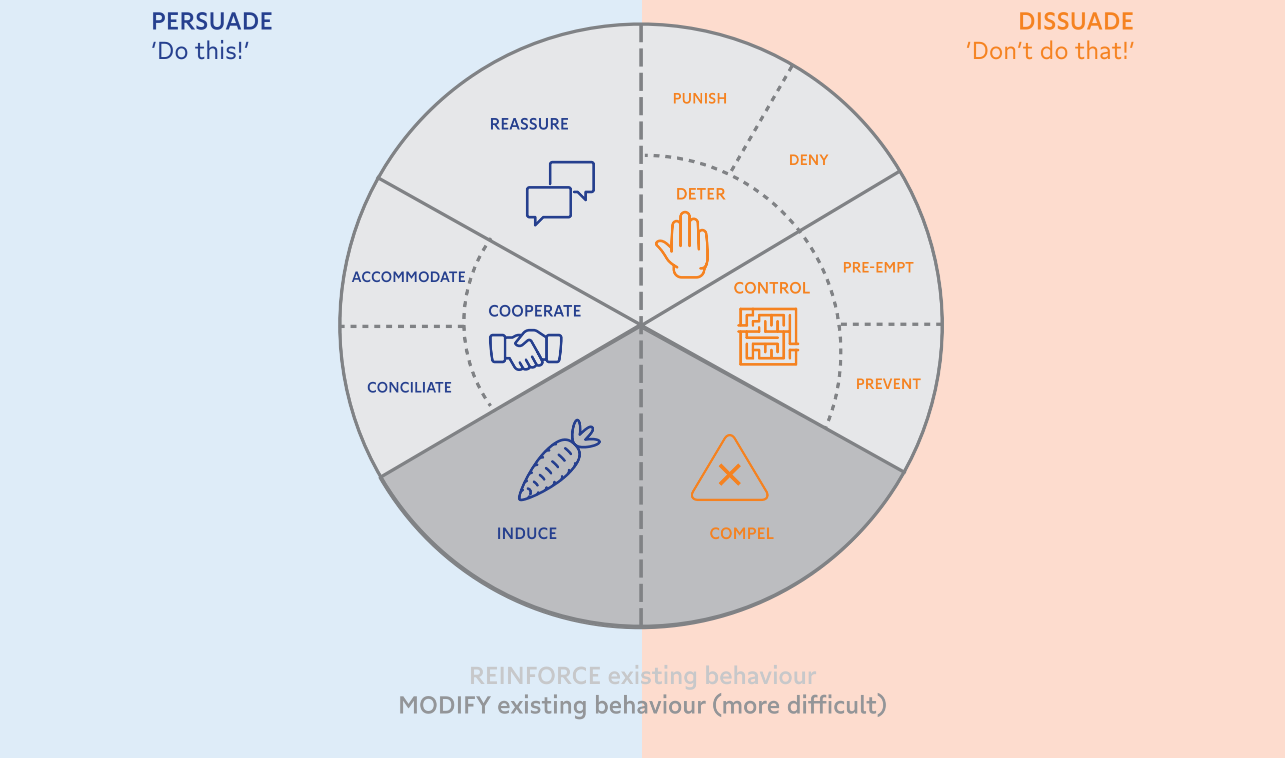
Given the evolving and dynamic nature of hybrid threats in an era of intensifying strategic competition, the risk of so-called 'wormhole escalation' (from low-level hybrid to conventional and nuclear escalation) is ever-present.[173] To combat this risk, nuclear and conventional deterrence should be maintained where possible through force superiority and escalation dominance. The role of these factors should not be underestimated – both to deter armed aggression and the most serious hybrid threats.[174]

5.2. Going beyond deterrence

Just as resilience is not a strategy (in itself), neither is deterrence. As Hybrid CoE's *Deterrence Playbook* already states: "deterrence as a strategy does not stand alone – it has to be in line with other strategies governments and institutions use to manage their external relationships".[175] Countering hybrid threats requires more than just deterrence for at least two reasons. First, deterrence has several inherent limits (see above). Second, in the case of ongoing hybrid threat campaigns, deterrence has de facto already failed to some extent. Other strategies are therefore required to complement and go beyond deterrence. A taxonomy of relevant strategies is shown in Figure 11 below.

[170] For example, in the context of Russia: "Nuclear weapons are the foundation of the country's national security and the ultimate guarantee of its strategic independence. But they are not an instrument for risky endeavors – they ensure that other powers do not engage in such endeavors against Russia." See: Eugene Rumer, 'The Primakov (Not Gerasimov) Doctrine in Action', Carnegie, 5 June 2019, https://carnegieendowment.org/2019/06/05/primakov-not-gerasimov-doctrine-in-action-pub-79254.
[171] Jacek Durkalec, 'Nuclear-Backed "Little Green Men": Nuclear Messaging in the Ukraine Crisis', Report (The Polish Institute of International Affairs, July 2015), 5, 17–19, https://www.files.ethz.ch/isn/193514/Nuclear%20Backed%20%E2%80%9CLittle%20Green%20Men%E2%80%9D%20Nuclear%20Messaging%20in%20the%20Ukraine%20Crisis.pdf.
[172] As one analyst of Russian 'hybrid warfare' puts it: "Military power is the necessary enabler of hybrid warfare. Hybrid tools can be an instrument of risk management when hard power is too risky, costly, or impractical, but military power is always in the background." See: Rumer, 'The Primakov (Not Gerasimov) Doctrine in Action'. See also: Durkalec, 'Nuclear-Backed "Little Green Men"', 5. As he suggests, Russia's campaign in Ukraine "was backed up by Russia's potential to use its full spectrum of military capabilities, including conventional and nuclear forces".
[173] Hersman, 'Wormhole escalation'.
[174] Wasser et al., 'Risky Business'.
[175] Kersanskas, 'Deterrence'.

Figure 11: Deterrence and beyond: a taxonomy[176]



This taxonomy is suggestive, not definitive. More views abound on going beyond deterrence. For example, Thomas Schelling saw deterrence as inherently defensive and compellence as offensive.[177] US scholar Alexander L. George sees compellence as comprising two parts: a defensive form (to stop or undo an action) and an offensive form (to give up something of value).[178] RAND's Paul K. Davis equates dissuasion and deterrence, suggesting a model for 'dissuasion by denial'.[179] Authors at the Hague Centre for Security Studies and RAND both take this idea further.[180] The MCDC Countering Hybrid Warfare project's framework identifies two other components that complement deterrence: detection and response.[181] RAND and CSIS outline comprehensive strategies that go beyond deterrence.[182] Yet all of these analyses agree on the need to go beyond deterrence to counter hybrid threats.

5.3. The further evolution of hybrid threats and deterrence

5.3.1. The evolution of hybrid threats

The evolution of deterrence will depend on how hybrid threats evolve in the prevailing strategic environment. As evolutionary biologists say,

[176] Adapted from ideas in: King, 'New Challenges', 2 (the influence strategy typology); Blechman et al., *Force Without War* (the 'modify vs reinforce' distinction); Sweijs et al., 'Reimagining deterrence' (the 'persuade vs dissuade' distinction). These strategies may rely on all available levers of power, not just military force.

[177] Schelling, *Arms and Influence* (2020), 69. He saw the problem of 'ambiguous aggression' (e.g. hybrid threats) as being solved primarily through compellence, not deterrence. This point is also made in: Monaghan, 'To change Putin's behaviour'; and Pettyjohn and Wasser, 'Competing in the Gray Zone'.

[178] Alexander L. George, *Forceful Persuasion: Coercive Diplomacy as an Alternative to War* (United States Institute of Peace Press, 1991).

[179]Paul K. Davis, 'Towards Dissuasion (Deterrence) by Denial', Working Paper (Rand, 2014), https://www.rand.org/content/dam/rand/pubs/working_papers/WR1000/WR1027/RAND_WR1027.pdf.

[180] Sweijs et al., 'Reimagining deterrence'; Michael J. Mazarr et al., 'What Deters and Why'.

[181] Monaghan et al., 'MCDC Countering Hybrid Warfare'.

[182] Morris et al., 'Gaining Competitive Advantage'; Hicks et al., 'By Other Means Part I'.

"everything is everywhere, but the environment selects." The trends that have contributed to the rise of hybrid threats seem set to continue – but discontinuities can also be expected. Trends in three areas – power, technology and interdependence – are worth noting.

Power

The shifting balance of regional and global power towards a more competitive, multipolar international system means more state actors will be more motivated and capable of challenging the status quo.[183]

The appetite for change of already active revisionists is unlikely to diminish in the near future,[184] and may well intensify where bolstered by economic growth and military expansion (e.g. China), or required by relative structural decline (e.g. Russia).[185] The question is whether they will seek change through hybrid threats or more drastic measures. Moreover, at some point, increasingly motivated and capable revisionists will 'break out' of the grey zone when they feel able to do so (as per the current crisis with an emboldened Russia).[186] One dilemma is whether to act now or later to prevent this from happening.[187]

Technology

As well as shifting among states, power is also diffusing within them. This trend is driven by new technology which gives sub-state actors and individuals more information, connectivity and tools.

Digital and communication technology has provided state and sub-state actors with more means to influence and threaten others in new ways that are often difficult to attribute or easy to deny.[188] This technology can open new fissures and frontlines across the whole of society, from cyber phishing attacks executed by and targeted at individuals, to disinformation battles played

[183] The distribution of power among states is an important factor in the stability of the international system. See: Kenneth Waltz, *Theory of International Politics* (McGraw-Hill, 1979). Although power is diffusing – both among states and towards non-state actors, including multinational and transnational organizations – states retain a relative monopoly on economic and military power. See: UK Ministry of Defence, 'Global Strategic Trends'. The most problematic state actors can be defined primarily by the extent to which they wish to revise or overturn the existing status quo. See: Linda Robinson et al., 'Modern Political Warfare', Research Report (RAND, 2018), 16, https://www.rand.org/pubs/research_reports/RR1772.html.

[184] Based on indicators such as rhetoric for change, capability to achieve it and actions taken. See for example: Dubik and Vincent, 'America's global competitions'. Given that North Korea's extreme revisionism is based primarily on the threat of a nuclear strike or retaliation, their challenge (while important) does not fit the hybrid threat paradigm – unlike the gradual but aggressive approaches of Russia in Europe, China in the South China Sea, and Iran in the wider Middle East.

[185] For views on the persistence of Russian revisionism despite (or because of) relative structural decline, see: Michael Kofman and Andrea Kendall-Taylor, 'The Myth of Russian Decline: Why Moscow Will Be a Persistent Power', *Foreign Affairs*, Nov/Dec 2021, https://www.foreignaffairs.com/articles/ukraine/2021-10-19/myth-russian-decline; Richard Connelly and Michael Kofman, 'What Putin Learned From the Soviet Collapse', *Foreign Affairs, 29 December 2021*, https://www.foreignaffairs.com/articles/russia-fsu/2021-12-29/what-putin-learned-soviet-collapse.

[186] In fact, successfully countering hybrid threats may be a case of 'be careful what you wish for', as revisionist actors who remain motivated are provided with the incentive to pursue more drastic measures to achieve change. See Monaghan, 'Countering Hybrid Warfare', 90.

[187] Jensen et al., 'Shadow Risk'.

[188] See for example: UK Ministry of Defence, 'Global Strategic Trends'.

out on social media.[189] As Henry Kissinger and his co-authors put it: "A central paradox of our digital age is that the greater a society's digital capacity, the more vulnerable it becomes."[190]

Emerging technologies such as artificial intelligence (AI) will accelerate these trends, changing power balances and enhancing the power of citizens, governments and militaries well beyond the advances already realized through the information revolution.[191]

Interdependence

With increasing interdependence in the international system, more states may be increasingly vulnerable to others in new and novel ways. The deepening of 'complex interdependence' between nations has been intensified through accelerating globalization across all spheres of life, from economic to cultural.[192] Although this has brought many benefits to many people, it also means that states are dependent on –and therefore vulnerable to – each other to an extent never seen before, and in ways they might not even know about. This increases both the target surface area and the level of ambiguity, opacity and surprise possible for future hybrid threats.

None of this suggests that armed conflict will become obsolete. In fact, as more nations grow their militaries, develop new military technology and adopt more competitive or confrontational postures towards each other, the risk of military conflict will only grow.[193]

However, should the strategic environment continue to be characterized in large part by both disincentives for revisionists to resort to major war — such as the preponderance of hard power belonging to the status-quo powers and the tempering effects of nuclear weapons — and incentives to retain a stake in the order — such as economic growth and status for emerging powers — then would-be revisionists are more likely to use hybrid threats to achieve measured aims, gradually over time, through a combination of means.[194]

While this trend has positive aspects – rather 'hybrid war' than real war – the increased range and intensity of hybrid threats, combined with the destabilizing effects of new technology, may lead to unintended and unpredictable escalation.[195]

5.3.2. Deterring future hybrid threats

The evolution of hybrid threats will have implications for deterrence. These can be examined through the 'three Cs'.

[189] For example: "digitized propaganda, disinformation and political meddling with a larger scope and impact than in previous eras. They are made possible by the expansiveness of the digital technology and network platforms on which these campaigns unfold". See: Henry Kissinger et al., *The Age of AI: And Our Human Future* (Little Brown and Company, 2021), 153.
[190] Kissinger et al., *The Age of AI*, 153.
[191] See for example: Payne, 'Artificial Intelligence', 23; and Michael C. Horowitz, 'Artificial Intelligence, International Competition, and the Balance of Power', *Texas National Security Review*, Volume 1, Issue 3 (May 2018): 36–57, https://doi.org/10.15781/T2639KP49.
[192] Richard Baldwin, *The Great Convergence: Information Technology and the New Globalization* (Belknap Press, 2016).
[193] See for example: James S. Johnson, 'Artificial Intelligence: A Threat to Strategic Stability', *Strategic Studies Quarterly* (Spring 2020), 17, https://www.airuniversity.af.edu/Portals/10/SSQ/documents/Volume-14_Issue-1/Johnson.pdf. As he states: "the increasingly competitive and contested nuclear multipolar world order will...increase escalation risks in future warfare between great military powers – especially China and the United States".
[194] Mazarr, 'Mastering the Gray Zone'.
[195] Hersman, 'Wormhole Escalation'.

Capability

As hybrid threats evolve to encompass the whole of digital and networked societies, so too will the capabilities required to deter them. A more complex threat environment will make predicting attacks and vulnerabilities more difficult, so nations may rely more on resilience.[196] Resilience best practice requires devolving action to the most suitable stakeholders – these will increasingly be private entities and individual citizens.

Advances in AI will help and hinder these efforts, "shaping all conflicts from the lowest to highest intensity and the smallest to largest scale", as well as society itself.[197] Because "the 'attack surface' of a digital, highly networked society will be too vast for human operators to defend manually…Countries, companies and even individuals should invest in fail-safes to insulate them from such scenarios".[198]

New technologies will provide new threats of punishment too, such as cyberattack or AI-enabled vulnerability detection.[199] The unequal development of emerging technology between major powers will offer some nations capabilities that others will not be able to afford or have access to. In the case of AI this could lead to a "Pax AI", where – as with nuclear weapons – some nations shelter under the extended deterrence umbrella of others.[200]

The risks of escalation and unintended effects will multiply as new technologies are developed and fielded.[201] For example, "AI increases the inherent risk of pre-emption and premature use escalating into conflict", yet "in contrast to the field of nuclear weapons, no widely shared proscription and no clear concept of deterrence (or of degrees of escalation) attend such uses of AI".[202] Advances in situational awareness technology may both enhance and undermine deterrence.[203]

Credibility

Denial by resilience measures pose less of a credibility problem than threats of punishment, which entail public support, cost absorption (e.g. for financial sanctions that also harm the deterrer), and escalation risk. Both will be affected by trends in risk appetite and resilience in Western nations, as well as emerging technology such as AI, which "changes the risks from using force, especially for casualty averse states, which are most likely to field it…[this] may actually provoke conflict by making it affordable

[196] On a more complex threat environment, for one example of the future range of hybrid threat capabilities, see: Monaghan, 'Countering Hybrid Warfare', 89.

[197] Payne, 'Artificial Intelligence', 8 and 19–20.

[198] Kissinger et al., *The Age of AI*, 164.

[199] Kissinger et al., *The Age of AI*, 158.

[200] Payne, 'Artificial Intelligence', 25.

[201] See for example Morgan, 'The State of Deterrence', 101: "This could readily generate severe reciprocal fear-of-surprise-attack problems, with opponents guessing about each other's capabilities and whether an attack is coming, each fearing the other is on the verge of gaining a crucial technological edge".

[202] Kissinger et al., *The Age of AI*, 155–165. See also: James S. Johnson, 'The AI-Cyber Nexus: Implications for Military Escalation, Deterrence, and Strategic Stability', *Journal of Cyber Policy*, Volume 4, Issue 3 (2019): 442–460, https://doi.org/10.1080/23738871.2019.1701693.

[203] Rebecca Hersman and Reja Younis, 'The Adversary Gets a Vote', CSIS, 27 September 2021, https://www.csis.org/analysis/adversary-gets-vote; Thomas G. Mahnken, 'Deterrence by Detection: A Key Role for Unmanned Aircraft Systems in Great Power Competition', CSBA, 14 April 2020, https://csbaonline.org/research/publications/deterrence-by-detection-a-key-role-for-unmanned-aircraft-systems-in-great-power-competition; Johnson, 'Artificial Intelligence', 22.

for hitherto risk-averse states. AI could deter aggression by adventurers seeking easy gains that are no longer below the threshold for intervention".[204]

The credibility of deterrence is also challenged by the complexity and unpredictability of the hybrid threat landscape. Hence one study advocates "some 'better roughly right than precisely wrong' multi-criteria decision-making approaches" to calculating the likely costs of deterrence measures.[205] A study by RAND argues for applying this uncertainty-centric approach to designing deterrence and influence strategies writ large.[206]

Communication

Deterrence relies on both understanding and conveying capabilities and intentions between actors. Future trends look set to profoundly complicate these efforts. To the extent that AI-enabled technologies feature in the future hybrid threat landscape, the deepest challenge may be philosophical, as analyses of adversary capabilities and intentions – and even the decisions that follow – involve non-human intelligence (on both sides).[207] The AI era risks moving the conduct of strategy in international affairs beyond human intention and understanding.[208] In this sense, "nuclear weapons were arguably less revolutionary than AI, in that they did not alter the psychological essence of strategic affairs".[209] For conventional military deterrence, AI "may alter cost-benefit calculations by removing the fog of war, by superficially imposing rationality on political decisions, and by diminishing the human cost of military engagement" – all of which may speed up the pace of coercive action beyond the point of human control and introduce fundamental uncertainty into comprehension and signalling.[210]

Signalling and interpretation problems are also exacerbated by emerging technology.[211] Another complicating factor regarding AI and other emerging technologies is that, as the pace and extent of their development remains an unknown quantity between states, perception (as opposed to reality) will have an outsized effect on behaviour.[212] For example, while advances in situational awareness technology may enhance efforts to understand adversary capabilities, these could also have destabilizing 'arms-race' effects.[213]

5.4. Deterring hybrid threats: towards a post-modern, 'fifth wave' of deterrence theory and practice?

5.4.1. Four waves of deterrence theory and practice

The late US scholar Robert Jervis characterized the evolution of deterrence theory and practice

[204] Payne, 'Artificial Intelligence', 25.
[205] Sweijs et al., 'Reimagining deterrence'.
[206] Paul K. Davis et al., 'Influencing Adversary States: Quelling Perfect Storms', Research Report (RAND, 2021), https://doi.org/10.7249/RRA161-1.
[207] Kissinger et al., *The Age of AI*, 161.
[208] Ibid., 139.
[209] Payne, 'Artificial Intelligence', 7.
[210] Alex Wilner and Casey Babb, 'New Technologies and Deterrence: Artificial Intelligence and Adversarial Behaviour', Chapter 21 in *Annual Review*, ed. Frans Osinga and Tim Sweijs (T.M.C. Asser Press: The Hague, 2020), 402.
[211] Evan Braden Montgomery, 'Signals of strength: Capability demonstrations and perceptions of military power', *Journal of Strategic Studies*, Volume 43, Issue 2 (2020): 309–330, https://doi.org/10.1080/01402390.2019.1626724.
[212] Johnson, 'Artificial Intelligence', 17.
[213] Hersman and Younis, 'The Adversary gets a Vote'.

Table 3: Five waves of deterrence theory and practice

Wave	Empirical focus	Interpretive focus	Actor focus	Deterrence focus (denial vs punishment)	Domain focus
First	How to deter nuclear use?	-	State	Deterrence by punishment (e.g. MAD)	Nuclear weapons
Second	How to deter rational military actors?	-	State	Deterrence by punishment	Military strategy
Third	How to deter non-rational military actors?	The formation and role of norms, identity, non-rational behaviour	State	Deterrence by punishment	Military strategy
Fourth	How to deter actors with no return address? (E.g. terrorists, hackers)	Why do people become terrorists?	Non-state	Deterrence by punishment (some denial)	Military strategy; non-military tools (e.g. economic, cultural – deradicalization, societal resilience)
Fifth	How to deter hybrid threats?	Whose security? Who is deterring who?	State; sub-state	Deterrence by denial (some punishment)	Non-military; whole of government and society; "threats more annoying than deadly"

in 'waves'.[214] The first three waves can be characterized simplistically as being focussed on nuclear deterrence (first), rational choice and game theory (second), and 'non-rational' decision-making (third). All three were state-centric and primarily concerned with military-strategic matters.

A subsequent fourth wave has been characterized by a shift towards deterring 'asymmetric' threats from non-state actors and the recognition of a broader concept of deterrence that goes beyond military means.[215] Fourth wave deterrence theory has also been credited with incorporating the constructivist or interpretivist perspectives sorely lacking in the first three waves, which took states' interests and motivations as given.[216]

Table 3 compares the established four waves of deterrence theory and practice with a putative fifth wave, which is introduced and further explained below.[217]

[214] Robert Jervis, 'Deterrence theory revisited', *World Politics*, Volume 31, Issue 2 (1979): 289–324, https://doi.org/10.2307/2009945.

[215] See for example: Jeffrey W. Knopf, 'The fourth wave in deterrence research', *Contemporary Security Policy*, Volume 31, Issue 1 (2010): 1–33, https://doi.org/10.1080/13523261003640819; Amir Lupovici, 'The Emerging Fourth Wave of Deterrence Theory –Toward a New Research Agenda', *International Studies Quarterly*, Volume 54, Issue 3 (September 2010): 705–732, https://www.jstor.org/stable/40931133.

[216] Lupovici, 'The Emerging Fourth Wave', 710–712.

[217] Table adapted from Sweijs and Osinga, *Annual Review*, 526; Lupovici, 'The Emerging Fourth Wave'; Morgan, 'The State of Deterrence'.

5.4.2. A putative fifth wave of deterrence

The prospect of a fifth wave of deterrence theory and practice has been floated by a handful of authors.[218] Although it has not been labelled as such, there is an established literature on 'cross-domain deterrence' that can be considered part of this trend.[219] This field widens the concept of deterrence across the breadth of hybrid threats.

No detailed characterization of a putative fifth wave of deterrence theory and practice exists as yet.[220] An initial attempt is made to sketch out its possible main features below, in terms of both continuity (from previous waves) and change (new features).

Continuity

Deterrence remains – for now – a fundamentally psychological endeavour to manipulate the decision calculus (through risk, costs and incentives) of others to prevent them from pursuing undesirable courses of action. Preventing the use of military – and nuclear – force remains the primary objective of deterrence given the high cost of failure. The threat of military force also remains the sine qua non of deterrence due to its potency. While non-state actors remain relevant to the fifth wave, they are no longer of prime concern as state actors return to the stage in an era of multipolar competition. Importantly, consensus remains – even intensifies – over the central role of deterrence in security strategy to prevent undesirable outcomes, from the erosion of personal security to large-scale conflict.

Change

Although the deterrence of military threats remains the most important deterrence objective (due to the potential costs of failure), the main focus is on deterring "threats more annoying than deadly".[221] These are predominantly non-military hybrid threats that span the breadth of government and society, increasingly blurring the distinction between international and domestic, collective and individual. The complexity, variety and volume of threats, actors and targets – and therefore the scope of deterrence action – is unprecedented in previous waves. While the context of interstate competition will drive the security and deterrence environment, the reality of power diffusion (within states) and the connectedness of citizens necessitates a large sub-state component – deterrence will be less about elites managing crises and more about whole societies maintaining their individual (personal) and collective (sub-state and state-level) freedoms.

As a result of these new features of the deterrence environment, the emphasis of deterrence strategy will shift away from punishment towards denial through resilience. The relevant levers of power and tools of deterrence action will be wielded less by the military and government

[218] Most notably by Sweijs and Osinga, *Annual Review*, 524–529. Tim Prior suggests "Applied resilience is becoming the cornerstone of security policy, and represents the fifth wave of deterrence" (see: Prior, 'Resilience: The 'Fifth Wave', 77). Michael Ruhle proposes that "in short, the 'fifth wave' contends that the concept of deterrence can be adapted to reach far beyond existential military contingencies and military threats". He also cites Hybrid CoE's *Deterrence Playbook* (Kersanskas, 'Deterrence') as part of this trend. See: Michael Ruhle, 'In Defense of Deterrence', National Institute for Public Policy, April 27 2020, https://nipp.org/information_series/ruhle-michael-in-defense-of-deterrence-information-series-no-457/.

[219] See for example: Adamsky, 'Cross-Domain Coercion'; Mallory, 'New Challenges in Cross- Domain Deterrence'; Tim Sweijs and Samuel Zilincik, 'The Essence of Cross-Domain Deterrence', Chapter 8 in *Annual Review*, ed. Sweijs and Osinga (T.M.C. Asser Press: The Hague, 2020); Gartzke and Lindsay, *Cross-Domain Deterrence*.

[220] The most detailed effort is made by: Sweijs and Osinga, *Annual Review*, 526.

[221] Morgan, 'The State of Deterrence', 100–101.

and more by the whole of society, woven into the fabric of everyday life. 'The way we make war reflects the way we make wealth' – and so for deterrence. This development will open more doors for interpretivist inquiry into deterrence theory, as more actors and perspectives complicate the intersubjective context of threat formation and the meaning of 'security' (and therefore deterrence). This will broaden the relevance of non-military subfields of deterrence theory and practice, from crime to public health and theology.[222] Such broadening and complexity is the essence of hybrid threats.

Ultimately – fifth wave or not – the evolution of hybrid threats and the security environment will at the very least lead to a renaissance in deterrence theory and practice. This is already underway, due to a combination of the return of intense competition between states to the front and centre of the international stage, and the novelty and proliferation of deterrence into new areas of government and society.

5.4.3. The deterrence of everything, anti-war and the sixth wave

Just as some have described the coming era as involving the 'weaponisation of everything',[223] deterrence in the era of hybrid threats may become a post-modern case of the 'deterrence of everything'. Patrick Morgan characterizes this new deterrence context well:

> *"[W]e currently face threats more annoying than deadly, much harder to detect and much more complicated to deter. We give them much attention as the threats of the day and because they might become far more than just annoying."*[224]

On the one hand, this prospect might entail the unwelcome securitization of evermore aspects of international, domestic and private life.[225] On the other hand, the shift of deterrent focus onto "threats more annoying than deadly" may actually represent *progress* in international and human security. It may even be a form of 'anti-war': deterring hybrid war rather than actual war.[226]

Looking further into the future, the truly revolutionary implications of AI may invite a sixth wave of deterrence theory and practice – when the essence of deterrence moves beyond the manipulation of human decisions to the inscrutable logic of intelligent machines.[227]

[222] See for example Sweijs et al., 'Reimagining deterrence', 7: "in academic disciplines other than political science, including criminology, labor relations, public health, education, and religion." See also: Halas, 'NATO's sub-conventional deterrence'.

[223] Galeotti, *The Weaponisation of Everything*. See also: Thomas Wright, *All Measures Short of War: The Contest for the 21st Century and the Future of American Power* (Yale University Press, 2017).

[224] Morgan, 'The State of Deterrence', 100–101.

[225] See for example: Jaap de Wilde et al., *Security: A New Framework for Analysis* (Lynne Rienner Publishers, 1997); Thierry Balzacq, *Securitization Theory: How Security Problems Emerge and Dissolve* (Routledge, 2010); Rosa Brooks, *How Everything Became War and the Military Became Everything* (Simon and Schuster, 2017).

[226] According to 1990s futurists Alvin and Heidi Toffler, "anti-wars involve strategic applications of military, economic and informational power to reduce the violence so often associated with change on the world stage". Anti-wars "include actions taken by politicians, and even by warriors themselves, to create conditions that deter or limit the extent of war". See: Alvin and Heidi Toffler, *War and Anti-war*, 4.

[227] Kenneth Payne (Payne, 'Artificial Intelligence') suggests that there may only be two true 'revolutions' in human history: "The first revolution separates Homo sapiens from other primates, via a cognitive explosion some 100,000 years ago that brought about rich social interaction, language, the capacity for self-reflection and empathy with others, and the ability to make tools. These are the foundations of human strategy. A second revolution, now under way, is moving strategy beyond purely biological, human intelligence" (p. 11). See also: Kenneth Payne, *Strategy, Evolution and War: From Apes to Artificial Intelligence* (Washington DC: Georgetown University Press, 2018).

Author

Sean Monaghan is a visiting fellow in the Europe, Russia, and Eurasia Program at the Center for Strategic and International Studies, where he focusses on European security and defence. His career as a civil servant in the UK Ministry of Defence has focused on international defence policy, including NATO, the European Union, and the United States. In recent years, his work as a policy analyst has seen him contribute to the United Kingdom's Integrated Review and lead multinational research projects, including the MCDC Countering Hybrid Warfare project.

Hybrid CoE

The European Centre of Excellence
for Countering Hybrid Threats