RUSI
Royal United Services Institute
for Defence and Security Studies

Emerging Insights

Rethinking Cyber Deterrence in a Multipolar World

Louise Marie Hurel and Gareth Mott

August 2025

ACKNOWLEDGEMENTS

The authors would like to thank Microsoft for their ongoing support for and funding of this project. The authors are also especially grateful to the experts who generously shared their time and expertise through written feedback or participating in the workshop. Their insights are pivotal to the refinement of this paper.

EXECUTIVE SUMMARY

Geopolitical tensions in cyberspace are escalating. There is an urgent need to reassess how the cyber domain can support broader deterrence strategies. However, the effectiveness of deterrence in cyberspace remains contested among scholars and practitioners. While malicious cyber activity targeting critical national infrastructure (CNI) continues to mount – posing increasing risks to the national security of Western states[1] – it remains unclear whether deterrence measures have meaningfully reduced the frequency, scale and severity of these incidents.

Although there has been no 'catastrophic nationwide cyber attack', persistent low-level activity – particularly from Russia and China – has targeted a range of CNIs and sectors in the West. This trend risks being obscured by 'unrealised and unspecific scaremongering',[2] leaving policymakers ill-prepared to respond to evolving threats.

This paper balances existing prevailing scepticism about the feasibility of cyber deterrence against the growing political imperative to impose consequences – both cyber and non-cyber – on malicious actors. It explores the question: if a state cyber operation led to a Category 1 cyber incident – described by the National Cyber Security Centre as 'a cyber attack which causes sustained disruption of UK essential services or affects UK national security'[3] – with sustained threat to life, how could the UK and its allies deter an actor from attempting another breach?

This paper argues that cyber deterrence must be part of an integrated, cross-domain strategy. Deterrence should be understood as a continuum of prevention and response measures – cumulative, iterative, tailored and grey-zone oriented – drawing from lessons across multiple case studies. It

1. Kevin Poireault, 'UK Cyber-Attacks Surge as Threats Hit Harder, Warns NCSC', *Infosecurity Magazine*, 3 December 2024, <https://www.infosecurity-magazine.com/news/uk-cyberattacks-surge-ncsc/>, accessed 17 June 2025.
2. Ciaran Martin, 'Typhoons in Cyberspace', *RUSI Commentary*, 20 March 2025, <https://www.rusi.org/explore-our-research/publications/commentary/typhoons-cyberspace>, accessed 10 June 2025.
3. National Cyber Security Centre (NCSC), 'Categorising UK Cyber Incidents', 23 August 2023, p. 5, <https://www.ncsc.gov.uk/information/categorising-uk-cyber-incidents>, accessed 15 May 2025.

particularly considers the implications of cyber operations 'pre-positioning' for disruptive or destructive attacks.

KEY RECOMMENDATIONS

- Adopt a pragmatic framing of cyber threats, integrating lessons from cross-sector crisis response and developing tailored and actor-specific deterrence strategies.
- Balance strategic ambiguity and credible signalling – particularly in determining the red lines of cyber operations and when crossing them may constitute a threat or use of force under international law.
- Break inertia and consider a full range of deterrence responses – including swifter, timely and proportionate action to sub-threshold incursions,[4] and complementary measures across economic, diplomatic or even covert domains.

This analysis is based on a rapid evidence assessment and expert consultations. A second RUSI research paper will explore how to frame the effectiveness of different deterrence approaches across case types and threat actors. That paper will also look closely at specific case studies.

INTRODUCTION

At NATO's Conference on Cyber Conflict (CyCon) in May 2025, Emily Goldman, senior US cyber strategist for the National Security Agency, announced further details of the US's evolving approach to deterring malicious cyber activity. The message was clear: 'instead of responding and reacting to the opponent's last move, we want to move proactively, to constrain their options before they act. To interrupt, to frustrate, to complicate their strategy for victory across all geopolitical conditions. We need to seize and hold the initiative and not cede the initiative.'[5] The speech signalled the US government's ambition to move from 'restraint' and 'threatening to act' to a more proactive approach. It is symptomatic of the current highly contested threat landscape where cyberspace is an arena to disrupt adversaries, protect national security, conduct espionage and set conditions ahead of future conflict.

The US is not alone in its evolving posture. In June 2025, the UK published its Strategic Defence Review (SDR). The once-in-a-decade document sets the vision for UK Defence's priorities in the years to come and similarly changes the narrative: 'moving to warfighting readiness to deter threats and strengthen

4. Here, 'sub-threshold' refers to incidents that do not meet the threshold of an act of war.
5. Emily Goldman, 'Dr Emily Goldman - Senior US Cyber Strategist, National Security Agency', speech given at CyCon 2025, 28 May 2025, YouTube, <https://youtu.be/P_L1ZN5PtM8?si=Wxs5Mvu2yjVxGZIH>, accessed 4 June 2025.

security in the Euro-Atlantic'.[6] In practice, this means setting forth a tangible plan for a deterrence that is institutionally and operationally 'integrated by design'. It also entails a shift: from a domain-exclusive approach to cyber, to the proposed Cyber and Electromagnetic Command (CyberEM), whose purpose is supporting a more proactive footing in this domain and ensuring cross-domain coherence.

Such developments have not emerged without reason. Western governments have gradually sought to bolster cyber deterrence strategies through the development of policies, frameworks, exercises, sanctions, operations and public cyber attribution statements. However, the drumbeat for further deterrence is growing ever louder. This momentum is driven by the intensification of conflict in cyberspace and a growing recognition of the need for greater integration across domains and government sectors. It also reflects an increasingly multipolar and contested geopolitical landscape. Crucially, the scale of cyberattacks and long-term pre-positioning by certain threat actors – including overt and tacit state activity – has further propelled cyber threats to the top of the national security agendas of Western governments.

'Cyber deterrence' has conventionally focused on deterrence using cyber effects. Now, given the relationship between cyber and wider geopolitics, it makes sense to expand this concept to include deterrence of malicious cyber activity by using all levers of government (diplomatic, economic, military).[7]

However, the feasibility and effectiveness of deterrence in cyberspace has been contested among scholars and practitioners for some time. The community has therefore been divided on how to even start a dialogue on strategies, let alone judge their effectiveness.[8] Certain perspectives highlight

6. Ministry of Defence (MoD), 'The Strategic Defence Review 2025 – Making Britain Safer: Secure at Home, Strong Abroad', 8 July 2025, <https://www.gov.uk/government/publications/the-strategic-defence-review-2025-making-britain-safer-secure-at-home-strong-abroad>, accessed 14 July 2025.
7. This paper uses the term 'cyber deterrence' to refer to the strategic signalling and disruption of an adversary's cost–benefit calculation (through kinetic and non-kinetic means) to the degree that it disincentivises malicious cyber behaviour from the attacker due to the increased likelihood of failure, the increased burden of time and resources required to conduct an attack, and/or the threat of significant reprisals in the event that the breach is successful (or possibly even attempted). Louise Marie Hurel, 'New Ways to Frame Responsible Cyber Behaviour Beyond the UN', *RUSI Occasional Papers* (May 2025), <https://www.rusi.org/explore-our-research/publications/occasional-papers/new-ways-frame-responsible-cyber-behaviour-beyond-un>, accessed 31 July 2025.
Also see Stefan Soesanto, *Cyber Deterrence Revisited* (Maxwell Air Force Base, AL: Air University Press, 2022).
8. Manuel Fischer, 'The Concept of Deterrence and its Applicability in the Cyber Domain', *Connections* (Vol. 18, No. 1/2, 2019), pp. 69–92; Erica Lonergan and Mark Montgomery, 'What is the Future of Cyber Deterrence?', *SAIS Review of International Affairs* (Vol. 41, No. 2, 2021), pp. 61–73; Peter Pijpers and Kraesten

that one purpose of cyber deterrence is to, over time, demonstrably decrease the number of offensive cyber incidents that states conduct. However, measuring effectiveness is challenging: it is difficult to credibly establish causality between deterrence measures and particular outcomes. Even when deterrence strategies – such as naming and shaming, sanctions (for example, seizure of assets and travel bans) or effects-based operations – are part of the state-based toolbox, that does not necessarily mean that the '3 Cs' of deterrence (capability, credibility and communication) have been implemented or are effective.[9]

Although it is challenging to operationalise and measure, cyber deterrence remains a critical component of a state's objective to achieve its defence and national security interests. It is clear that policy lenses are needed to distinguish 'unrealised and unspecific scaremongering'[10] from the concerning and specific cyber threats that need to be deterred in a tailored and systematic manner. This is especially important given cases of state-sponsored actors conducting military and intelligence cyber campaigns against a range of CNIs – such as those of Chinese cyber threat actors Volt and Salt Typhoon targeting US networks.[11]

The next stage of this research – to be published in a second RUSI paper – evaluates deterrence interventions over a longer timeframe involving cumulative impacts and effects. This first paper considers a range of circumstances, including where: delivering cyber effects is part of a wider response toolkit; trial and error is part of the process; cyber effects are positioned within a broader set of threats (intentional and non-intentional as well as kinetic and non-kinetic); and the objective of the approach is to maintain a persistent limit to malicious cyber behaviour (slowing, degrading, narrowing and constraining the space for adversarial action). The results of this research point to the need for an approach that combines both compellence (compelling adversaries to take a specific course of action) and deterrence (dissuading adversaries from engaging in a certain activity).[12] Consequently, this paper advocates for cumulative and tailored approaches

---

Arnold, 'Rethinking Cyber Deterrence: Adapting to the Realities of the Digital Battlefield', *Journal of Strategic Security* (Vol. 18, No. 1, 2025), pp. 61–76; Tim Stevens, 'A Cyberwar of Ideas? Deterrence and Norms in Cyberspace', *Contemporary Security Policy* (Vol. 33, No. 1, 2012), pp. 148–70.

9. Matthias Schulze, 'Cyber Deterrence is Overrated', *SWP Comment* (No. 34, August 2019); Stefan Soesanto, 'After a Year of Silence, are EU Cyber Sanctions Dead?', *Lawfare*, 26 October 2021, <https://www.lawfaremedia.org/article/after-year-silence-are-eu-cyber-sanctions-dead>, accessed 27 May 2025.
10. Martin, 'Typhoons in Cyberspace'.
11. Erica Lonergan and Michael Poznansky, 'A Tale of Two Typhoons: Properly Diagnosing Chinese Cyber Threats', *War on the Rocks*, 25 February 2025, <https://warontherocks.com/2025/02/a-tale-of-two-typhoons-properly-diagnosing-chinese-cyber-threats/>, accessed 31 July 2025.
12. Uri Tor, '"Cumulative Deterrence" as a New Paradigm for Cyber Deterrence', *Journal of Strategic Studies* (Vol. 40, No. 1/2, 2017), pp. 1–26.

to deterring malicious cyber activities, using all available government tools to respond to both cyber and non-cyber threats that fall below the threshold of armed conflict. Further research is required to identify the modalities of such deterrence strategies. The second RUSI research paper will explore this in greater detail, including approaches, opportunities and potential risks.

To reinvigorate the debate for this paper, the authors explore a hypothetical question: if a state cyberattack led to a Category 1 cyber incident with sustained threat to life, how could the UK and its allies deter another breach? Following the National Cyber Security Centre's UK cyber incident categorisation framework, a Category 1 incident is defined as 'a cyber-attack which causes sustained disruption of UK essential services or affects UK national security, leading to severe economic or social consequences or to loss of life'.[13] While the paper does not provide a comprehensive or prescriptive answer, it does make some recommendations to spur further policy research. This question is used to 'break inertia', enabling stakeholders to re-envisage a potential new or revised framework for cyber deterrence.

If a state cyberattack led to a Category 1 cyber incident with sustained threat to life, how could the UK and its allies deter another breach?

The authors undertook research in three stages: a rapid evidence assessment of the literature informed a baseline analysis of the state of play in the cyber deterrence debate to date; and two rounds of consultation with eight experts for data validation and additional data gathering. These experts, including academics, industry figures and former policy practitioners from the US and the UK, represented a cross-section of the cyber deterrence debate.

The paper has three sections. The first section provides a baseline for the response to the research question. It outlines the context of the overarching cyber deterrence debate to date and proposes key components for a cross-domain approach to the topic. The second section responds to the central question and shows how cyber deterrence consequences can be reframed as a spectrum of operations and impacts in the context of a broader deterrence campaign against adversaries. The final section makes recommendations for policymakers and stakeholders interested in deterrence strategies, and highlights challenges and opportunities for future research.

THE CYBER DETERRENCE DEBATES TO DATE

FIVE VIEWS OF CYBER DETERRENCE

A brief assessment of the conceptual contributions and challenges that have helped to open the 'saying and doing' gap in cyber deterrence is needed. Exploring these allows the gap to be narrowed. There are at least five major schools of thought that have emerged in policy and scholarly literature in the past years:

1. Nuclear deterrence analogies for cyber deterrence.
2. Cyber deterrence sceptics.

13. NCSC, 'Categorising UK Cyber Incidents'.

3. Persistent engagement.
4. Resilience over deterrence.
5. Cross-domain deterrence.

These are not formal 'schools' of thought, nor are they mutually exclusive. However, it is critical to understand them – including their limitations – to avoid falling into policy traps and to assess effective integrations of a cumulative and tailored approach to deterrence of malicious cyber activities.

NUCLEAR DETERRENCE ANALOGIES FOR CYBER DETERRENCE

The first school of cyber deterrence has sought to transpose concepts from nuclear deterrence to the cyber domain. Proponents of this approach to deterrence argue that the logic of mutually assured destruction can, under certain conditions, be applied to cyberattacks. In principle, a cyberattack on a CNI could be sufficiently severe to reach a threshold where a state is compelled to react with overwhelming cyber – or analogue – force. Proponents of this perspective view deterrence as effective when it has an absolute effect of stopping a certain action.[14] It also suggests that it is necessary to clearly signal red lines to adversaries and to develop a suite of retaliatory capabilities that establish deterrence.

However, there are policy and conceptual risks of comparing cyber to nuclear capabilities. Cyber capabilities are far less damaging than thermonuclear weapons. As such, this brings into question whether cyber can produce the same credible threat of retaliation as a nuclear weapon. Additionally, cyber capabilities are uniquely transitory (they are rendered less useful or even useless if the exploit is fixed). It is therefore difficult to materially display a cyber capability in the same way that a state can with its nuclear assets.

CYBER DETERRENCE SCEPTICS

A second school of thought questions whether it is at all possible to deter state-led cyber operations and other malicious activity in cyberspace. These sceptics argue that deterrence theory has been erroneously applied to cyberspace and is rooted in the historical securitisation of cyberspace as a military domain. They argue that espionage and intelligence – rather than military conquest – analogies are more suited to cyberspace. This approach therefore limits or eliminates the scope for a conventional reading of deterrence by punishment.[15] While low-intensity, persistent attacks in cyberspace are prevalent, these are below the threshold of armed conflict and, according to adopters of this school, are not acts that would typically require stringent deterrence.

14. Tor, '"Cumulative Deterrence" as a New Paradigm for Cyber Deterrence'.
15. Jon R Lindsay, 'Cyber Conflict vs. Cyber Command: Hidden Dangers in the American Military Solution to a Large-Scale Intelligence Problem', *Intelligence and National Security* (Vol. 36, No. 2, 2021), pp. 260–78.

Sceptics note that some of the assumptions about deterrence – such as the ability to signal precise thresholds, and quickly attribute and demonstrate credible retaliation – are often absent in defending critical systems in cyberspace.[16] Adversaries can therefore exploit the ambiguity of thresholds and test the limits of sub-threshold activity, even when this technically subverts laws and undermines sovereignty – especially as there has not been a cyberattack that amounts to the use of force nor a shared interpretation of what that threshold is under international law. Additionally, cyberspace enables obfuscation of agency and, notably, the formal and/or tacit outsourcing of cyber operations to proxies.[17]

However, dismissing cyber deterrence is also unhelpful. It paralyses policy responses, creating a disconnect with the current political will for, and necessity of, deterrence measures. Moreover, given the evolving threat landscape and recent high-profile case studies of cyber operations (that is, long-term pre-positioning by hostile state actors) and improved technical capabilities (that is, faster and more precise attribution), there may be new opportunities to introduce effective deterrence measures based on the current context.

PERSISTENT ENGAGEMENT

A third – and more recent – school of thought favours an approach of persistent engagement. This approach follows from the argument that cyberspace is a realm of continuous interaction among adversaries and, therefore, is where cyber operations impose costs and shape behaviours over time. The US Department of Defense's 2018 Cyber Defence Strategy introduced the notion of persistent engagement. That strategy argued that US Cyber Command has a capacity and responsibility to engage with adversaries to create constant friction and degrade capabilities, thereby deterring malicious action through cumulative effects.[18]

As an alternative to deterrence, proponents of persistent engagement argue that cyberspace is not a domain of restraint and reaction, and therefore deterrence cannot be the central strategy to achieve national interests.[19] These proponents have spurred a debate on persistent engagement is a better paradigm of competition – focusing on interaction rather than solely on escalation. In this regard, they suggest that persistent engagement seeks

16. Martin C Libicki, *Cyberdeterrence and Cyberwar* (Santa Monica, CA: RAND, 2009); Stevens, 'A Cyberwar of Ideas?'.
17. William Akoto, 'Accountability and Cyber Conflict: Examining Institutional Constraints on the Use of Cyber Proxies', *Conflict Management and Peace Science* (Vol. 39, No. 3, 2022), pp. 311–32.
18. US Cyber Command, 'Cyber 101 – Defend Forward and Persistent Engagement', 25 October 2022, <https://www.cybercom.mil/Media/News/Article/3198878/cyber-101-defend-forward-and-persistent-engagement/>, accessed 19 May 2025.
19. Jason Healey, 'The Implications of Persistent (and Permanent) Engagement in Cyberspace', *Journal of Cybersecurity* (Vol. 5, No. 1, 2019).

to inhibit, rather than deter, the cumulative impact of malicious activity in a way that falls short of the equivalent effect brought by armed attack.

While its proponents define persistent engagement as distinct from deterrence, it is still useful to think about how this school of thought adds to the debate. They argue that conventional deterrence strategies still hold for cyber operations that could lead to Category 1 incidents (or effects equivalent to an armed attack) as states would have the right to respond with conventional force. Persistent engagement therefore complements, in their view, the debate by addressing sub-threshold malicious cyber activities.

Two contributions follow. First, persistent engagement assumes that, over time, operations short of armed conflict can have a strategic-level cumulative impact.[20] This is similar to this paper's view of cumulative deterrence – albeit persistent engagement distances itself from deterrence. Second, persistent engagement implies less reliance on ad hoc reactions to specific malicious cyber operations, instead proposing a campaigns-based approach – which highlights the iterative and presumably interactional nature of signalling and cost imposition. Some argue that such activity should be carefully calibrated given the risk of escalation.[21]

RESILIENCE OVER DETERRENCE

Another perspective rejects the centrality of deterrence altogether. Instead, this school proposes that states prioritise cyber resilience.[22] It argues that rather than attempting to prevent attacks – an unrealistic goal in an environment of constant probing and penetration – efforts should focus on building (and maintaining) systems that can absorb, adapt to and recover from attacks with minimal disruption. Proponents contend that resilience reduces the attractiveness of cyberattacks by denying attackers the impact that they seek – in effect, a form of deterrence by denial.[23] A range of measures can be used to increase resilience, including (but not limited to):

Efforts should focus on building (and maintaining) systems that can absorb, adapt to and recover from attacks with minimal disruption

20. Michael P Fischerkeller and Richard Harknett, 'Persistent Engagement, Agreed Competition, and Cyberspace Interaction Dynamics and Escalation', *Cyber Defense Review* (2019), pp. 268–87.
21. Jacquelyn G Schneider, 'Persistent Engagement: Foundation, Evolution and Evaluation of a Strategy', 10 May 2019, *Lawfare*, <https://www.lawfaremedia.org/article/persistent-engagement-foundation-evolution-and-evaluation-strategy>, accessed 27 May 2025.
22. Mika Kerttunen, 'Deterrence a Naked Emperor', 13 September 2020, *Directions* blog, <https://eucyberdirect.eu/blog/deterrence-a-naked-emperor>, accessed 27 May 2025.
23. Erica Borghard and Shawn Lonergan, 'Deterrence by Denial in Cyberspace', *Journal of Strategic Studies* (Vol. 46, No. 3, 2021), pp. 1–36; Gavin Wilde, 'Russia's Countervalue Cyber Approach: Utility or Futility?', Carnegie Endowment for International Peace, 5 February 2024, <https://carnegieendowment.org/research/2024/02/russias-countervalue-cyber-approach-utility-or-futility>, accessed 16 May 2025.

segregation of networks; organisational preparedness; secure backups; and access to rapid incident response capabilities.

However, if this framing is applied exclusively, it shifts the burden almost entirely on to the defender and their third parties – letting the attacker off the hook. A purely resilience-focused approach may potentially embolden attackers who believe their action will carry no political or strategic cost. It also does not respond to the political appetite to impose costs beyond denying ease of access to systems or deployment of capabilities.

CROSS-DOMAIN DETERRENCE

A fifth school of thought, cross-domain deterrence, views cyber deterrence not as a standalone challenge, but as one part of a broader state toolkit involving multiple domains (that is, military, economic and diplomatic).[24] This perspective holds that cyberattacks can be deterred through retaliatory threats or actions in other domains. These may include conventional military strikes, sanctions or legal indictments. By expanding the menu of response options beyond cyberspace, cross-domain deterrence enhances the credibility and flexibility of deterrent postures. It acknowledges the limitations of cyber-for-cyber responses – especially when involving rivals with asymmetric capacities and vulnerabilities in cyberspace – and instead favours a full-spectrum response to impose costs on malicious actors.

While cross-domain deterrence may increase a state's flexibility to signal and incur prospective costs on adversaries, it also assumes a degree of coordination and intentionality in applying deterrence strategies across other areas of government – such as space, economic policy and diplomacy – which remains one of the biggest challenges for policymakers. A full-spectrum view of cyber deterrence requires governments to strengthen their ability to manage risks of escalation and miscalculation in an integrated manner, both across government agencies and in cooperation with the private sector.[25] Cross-domain deterrence also requires: an awareness of the strengths and weaknesses of different means of coercion; a careful assessment of how combining these tools (and their respective strengths and weaknesses) affects the credibility and effectiveness of deterrence and compellence; and a judicious assessment of proportionality and observance of states' international obligations.[26]

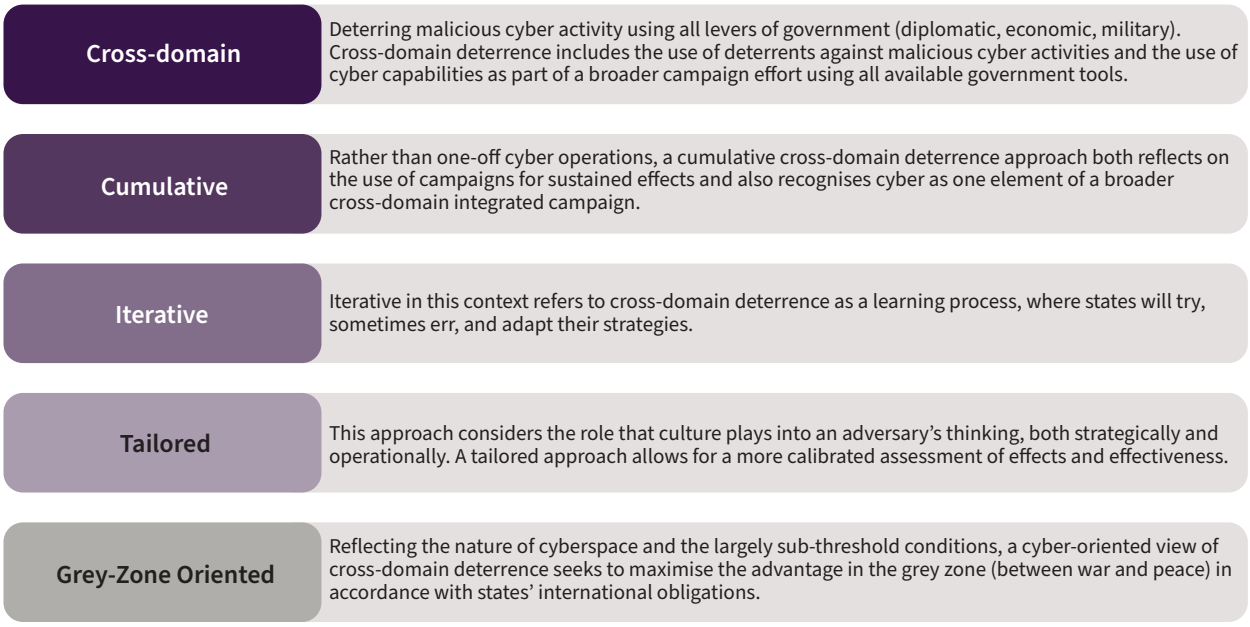
AN INTEGRATED VIEW OF CYBER DETERRENCE

Despite the challenges, and as the next sections show, thinking about a cumulative and tailored approach to cross-domain deterrence should be at the forefront of government thinking. Some countries are becoming more

24. Jon R Lindsay and Erik Gartzke (eds), *Cross-Domain Deterrence: Strategy in an Era of Complexity* (Oxford: Oxford University Press, 2019).
25. Nori Katagiri, 'Two Explanations for the Paucity of Cyber-Military, Cross-Domain Operations', *Journal of Cybersecurity* (Vol. 8, No. 1, 2022), pp. 1–10.
26. Lindsay and Gartzke (eds), *Cross-Domain Deterrence*.

vocal about adopting a similar approach, but this does not mean it is a reality.[27] Moreover, moving from words to action will require more legwork if adversary action by Russia, China, Iran, North Korea and others is to be deterred in cyberspace. Figure 1 provides a summary of key components.

Figure 1: Key Components of a Cyber-Oriented View of Cross-Domain Deterrence



Source: The authors.

REASSESSING CYBER DETERRENCE: GRADATION OF DETERRENCE EFFECTIVENESS

While the five prevailing views on cyber deterrence reflect a protracted and fragmented discourse, the policy appetite for credible, practical and careful actions remains strong.

Policymakers are encouraged to consider an approach grounded in cumulative deterrence, underpinned by two analytical exercises.

The first is to view cyber deterrence as a spectrum of prevention and response measures (from low- to high-impact measures) based on lessons learned from existing cases. The second is to position cyber disruptions within a broader non-cyber scale of disruptions (that is, like that for natural disasters) to understand the systemic impact that cyber has in relation to other catastrophic disruptions. This second exercise allows for a proper

27. Goldman, 'Dr Emily Goldman - Senior US Cyber Strategist, National Security Agency'; MoD, 'The Strategic Defence Review 2025 – Making Britain Safer'; Australian Government, Department of Home Affairs, '2023–2030 Australian Cyber Security Strategy', 2023; Alex Wilner, *The Many Shades of Canadian Deterrence* (Calgary: Canadian Global Affairs Institute, 2022).

calibration of preparedness to respond and act. Under such an approach, cyber is not seen through a specific lens, but is instead part of a broader portfolio of diplomatic and strategic engagement between states.[28] The ideal outcome is for policymakers to be able to apply deterrence tools as part of a 'tailored' cumulative campaign.[29] That is, long-form deterrence campaigns could be optimised if they were tailored for use against specific states and actors.

Both exercises rest on the premise that political will and context are arguably the most decisive factors for the selection of deterrence mechanisms and changes in posture. Figure 2 illustrates a simplified spectrum of indicative cyber operations to date, including low-, medium- and high-impact examples.

First, there are low-impact cases – those with minimal or no immediate disruption to networks or services per se, but which nonetheless still carry strategic significance. A key example is 'pre-positioning': broadly, the acts that allow a state to infiltrate and establish a foothold in technology and equipment, which then allow it to commit an act of sabotage at a later date.[30] In the context of cyber security, pre-positioning has also included the act of installing malware or introducing vulnerabilities into digital systems without activating the payload.[31] Unlike cyber espionage, which includes some form of data exfiltration, pre-positioning is about maintaining access without revealing the activity and/or the infiltrator's intentions. Although pre-positioning might be a prelude to greater-impact activity, it would probably be difficult to meaningfully implement a deterrence regime restricted to cyber actions against it. Activities such as the identification and remediation of vulnerable access points that are exploited by an adversary might be a temporary strategy of denying access. However, these are insufficient to shift behaviour and stop adversaries from looking for other access points.

Both Western and non-Western governments have reportedly engaged in pre-positioning activities. Although pre-positioning is low impact when strictly

28. Some of the literature on escalation management also reflects on intentional and unintentional effects in cyber and more broadly. See Forrest E Morgan et al., *Dangerous Thresholds: Managing Escalation in the 21st Century* (Santa Monica, CA: RAND, 2008).
29. Jeffrey S Lantis, 'Strategic Culture and Tailored Deterrence: Bridging the Gap Between Theory and Practice', *Contemporary Security Policy* (Vol. 30, No. 3, 2009), pp. 467–85; Franklin D Kramer and Melanie J Teplinsky, 'Cybersecurity and Tailored Deterrence', Atlantic Council Issue Brief, December 2013, <https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/cybersecurity-and-tailored-deterrence/>, accessed 4 August 2025.
30. HM Government, 'Sabotage: National Security Bill Factsheet', updated 24 June 2025, <https://www.gov.uk/government/publications/national-security-bill-factsheets/sabotage-national-security-bill-factsheet>, accessed 14 July 2025.
31. Juliet Skingsley, 'Cyber-Rattling: Can "Pre-Positioning" in Cyberspace Amount to a Threat of the Use of Force under Article 2(4) of the United Nations Charter?', *Journal on the Use of Force and International Law* (Vol. 11, No. 1/2, 2024), pp. 50–86.

assessed against its actual disruption and destruction of data or networks, its broader implications for research and policy warrant attention. First, when done at scale or in highly critical sectors – for example, in the cases of Volt and Salt Typhoon in their activities in the US – pre-positioning signals an actor's presence once discovered. The demonstration of an adversary's capabilities has potential psychological effects on the targeted country. Sustained performance of pre-positioning might create and consolidate heightened perceptions of uncertainty over the vulnerability of networks. Second, public communication strategies to condemn actions perpetrated by adversaries have limited and potentially contradictory effects. On the one hand, public condemnation shows discontent and unacceptability of conduct that can serve as justification for retaliation. On the other, public shaming may have immediate adverse effects and further embolden an adversary, especially as such activities are seen only as 'unacceptable' but are not deemed illegal under international law (although they may be under domestic law). Even so, the short-term morale boost might be an acceptable trade-off for the targeted state if growing collective displeasure with pre-positioning helps draw a more credible red line.

At the other end of the spectrum is a high-impact case – a 'severe catastrophic attack' – where a cyberattack results in massive kinetic impact: economic disruption and/or a high number of casualties, with direct threats to national security. It should be emphasised that, as a rule of thumb, it seems unlikely that cyberattacks would have the same impact as catastrophic kinetic equivalents – at least so far. Even where large-scale cyber disruption has impacted critical societal systems, it should be possible to remedy (although not necessarily immediately).[32] There is significant variability in the scale, impact and nature of an incident that meets the Category 1 designation. An impacted state may treat a cyber breach that is equivalent to a conventional strike as either above or below the threshold, depending on the specifics of the breach and its wider context. It is therefore possible to envisage an incident that is so severe – for instance, with irrefutable threat to life – that a government may choose, or feel compelled, to treat it as an above-threshold incident.

Even where large-scale cyber disruption has impacted critical societal systems, it should be possible to remedy

Between the two poles are medium-impact cases. This is a space of persistent, sub-threshold cyber activity with ambiguous impacts and attribution. Here, the potential for reinvigorating cyber deterrence is most acute. Rather than plan for extreme scenarios 'in the waiting', states must develop adaptive deterrence strategies for this middle ground, where the balance of ambiguity, signalling and tailored countermeasures might be more effective in shaping adversary behaviour.

32. Tom Johansmeyer, 'How Reversibility Differentiates Cyber from Kinetic Warfare: A Case Study in the Energy Sector', *International Journal of Security, Privacy and Trust Management* (Vol. 12, No. 1, 2023), pp. 1–14.

Table 1: Spectrum of Cyber Operations and Deterrent Impact

 **Low Impact**	 **Medium Impact**	 **High Impact**
In cases of pre-positioning, governments aim to signal concern and displeasure with such activity, but their deterrent responses are often limited to naming and shaming, advisories, and discovering and patching compromised networks.	The examples below show a mix of non-state, presumably (yet inconclusively) state-affiliated, and state-led cases that show the limitations and possibilities of deterring through or as a result of a cyber activity.	In the examples below, real-world incidents have been extrapolated to reflect on whether, with some changes, they might have achieved the level of use of force and thus demanded an exceptional response/deterrent.
Russia Pre-Positioning The Russian Federation, including affiliated actors, has conducted pre-positioning operations against CNI and CNI-adjacent systems in the US and allied states. In some cases, this activity appears to have been delegated by the GRU (Russian military intelligence) to associated threat groups.[33]	**Predatory Sparrow** Predatory Sparrow is an Israel-linked hacktivist group that has consistently targeted Iranian infrastructure since 2021. Activity took place in the context of Iranian-Israeli respective campaigns. Sparrow's campaigns have disrupted petrol stations and steel companies, among other sectors. These campaigns have been relatively targeted. The group has also engaged in signalling by publicising its activities. This includes the publishing of screenshots of code relating to leaks and disruptions to substantiate credibility and reputation.[34]	**Stuxnet 'Gone Nuclear'** Malware discovered in 2010 arguably deployed as a joint operation between the US and Israel against Iran's Natanz nuclear enrichment plant.[35] While originally it was contained, in retrospect it is relevant to consider the risk of escalation had a significant threat-to-life or ecological incident occurred.

33. Andy Greenberg, 'Hackers Tied to Russia's GRU Targeted the US Grid for Years, Researchers Warn', *Wired*, 24 February 2021, <https://www.wired.com/story/russia-gru-hackers-us-grid/>, accessed 1 August 2025.
34. Andy Greenberg, 'How a Group of Israel-Linked Hackers has Pushed the Limits of Cyberwar', *Wired*, 25 January 2025, <https://www.wired.com/story/predatory-sparrow-cyberattack-timeline/>, accessed 1 August 2025.
35. Kim Zetter, *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon* (New York, NY: Crown, 2015).

 Low Impact	 Medium Impact	 High Impact
US Pre-Positioning The US has been reported to have positioned reconnaissance and offensive tools in the Russian power grid. Attributed to the US Cyber Command and the NSA, this activity aligned with the adoption of a 'persistent engagement' approach.[36]	**SONY Picture** In 2014, the North Korea-based Lazarus Group deployed wiper malware on Sony Pictures networks and systems, stealing sensitive data and data relating to upcoming releases.[37] The attack was undertaken in reaction to the release of the movie *The Interview*, which depicted Kim Jong Un as emotionally unstable, manipulative and violent. The attack had a financial and business impact on Sony Pictures. There was also a psychological impact implicated by the threatening of terrorist attacks to auditorium viewers.	**Pakistan–India Escalation** Between 7 and 10 May 2025, Pakistan and India engaged in escalatory tit-for-tat kinetic military activity in the aftermath of the Pahalgam terrorist incident. The kinetic engagement included air-to-air combat, shelling, missile attacks and small-arms fire. There are allegations that state-linked and hacktivist hackers conducted cyber operations, including distributed denial of service (DDOS) attacks, targeting of phones of senior officials, and targeting of CNI. Offensive cyber activity may also have come from other jurisdictions. Looking ahead, it is possible that an intentionally or unintentionally severe cyber breach could result in unforeseen consequences in the context of adversarial and high-tension relationship between two nuclear-armed states.[38]
China Pre-Positioning China has reportedly engaged in the infiltration of US CNI, including communications, transportation, energy and water sectors. Some of this activity has been attributed to a purported state-sponsered hacking collective known as Volt Typhoon.[39]		

Source: The authors. Note: The cases outlined are illustrative and far from exhaustive. Cases were selected in response to peer review feedback and workshop discussions. The cases under 'high impact' are hypothetical scenarios, as no cyber operation in that category has occurred.

36. David E. Sanger and Nicole Perlroth, 'U.S. Escalates Online Attacks on Russia's Power Grid', *New York Times*, 15 June 2019, <https://www.nytimes.com/2019/06/15/us/politics/trump-cyber-russia-grid.html>, accessed 1 August 2025; Greg Myre, 'U.S. Reportedly Trying to Implant Malware that Could Sabotage Russia's Electrical Grid', *NPR*, 17 June 2019, <https://www.npr.org/2019/06/17/733497736/u-s-reportedly-trying-to-implant-malware-that-could-sabotage-russias-electrical->, accessed 1 August 2025.
37. Sean Gallagher, 'Inside the "Wiper" Malware that Brought Sony Pictures to its Knees [Update]', Ars Technica, 3 December 2014, <https://arstechnica.com/information-technology/2014/12/inside-the-wiper-malware-that-brought-sony-pictures-to-its-knees/>, accessed 1 August 2025.
38. Sameer Patil, 'Operation Sindoor and India-Pakistan's Escalated Rivalry in Cyberspace', *RUSI Commentary*, 20 June 2025, <https://www.rusi.org/explore-our-research/publications/commentary/operation-sindoor-and-india-pakistans-escalated-rivalry-cyberspace>, accessed 1 August 2025.
39. Cybersecurity and Infrastructure Security Agency, 'PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure', 7 February 2024, <https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a>, accessed 1 August 2025.

A focus on the middle ground moves away from an unhelpful framing of the hypothetical 'big event' while serving two important functions. First, operations (and their impacts) can be mapped according to their gradation of severity and objectively compared to non-cyber counterparts. Ransomware threats, for example, have seen large economic impacts, but on their own their impacts are still limited and insufficient to amount to an act of war.[40] This leads to the second point: a 'menu' of pre-emptive and reactive responses under a cumulative deterrence view can be proposed and assessed on the basis of their potential impacts and effectiveness against particular actors, their contextual dependencies and their drawbacks. In line with a cross-domain approach, the menu should include both cyber and non-cyber options. Policymakers should also consider the questions in Table 1 – these are by no means exhaustive.

Table 2: Menu of Pre-Emptive and Reactive Responses

Variables for Assessing Pre-Emptive and Reactive Responses	Guiding Questions
Potential impact	• What are the primary and secondary targets/ audiences? • What has the attacking state signalled? • What has been targeted? • Has any protected entity been targeted? • What are the potential impacts? • When will the impacts be realised? • Are the impacts proportionate or disproportionate to the nature of the threatened or realised incursion?
Potential effectiveness	• How will the adversary view the activity? • Will the activity be undertaken in a suitable timeframe? • Does the activity impact the adversary's behaviours and/or capabilities?
Contextual dependencies	• How does the activity fit into a wider deterrence campaign against the adversary? • What are the domestic, cultural, regional and international conditions that may influence the impact, effectiveness and/or drawbacks of the activity?
Potential drawbacks	• What resourcing is required? • What are the reputational risks? • What are the risks of escalation? • Could there be collateral impacts?

Source: The authors.

40. Tom Johansmeyer, 'Why Natural Catastrophes Will Always be Worse than Cyber Catastrophes', *War on the Rocks*, 4 April 2024, <https://warontherocks.com/2024/04/why-natural-catastrophes-will-always-be-worse-than-cyber-catastrophes/>, accessed 20 May 2025.

Importantly, as middle-ground cyber incursions are sub-threshold, 'one-shot' responses (whether signalled or actioned) may be poorly aligned with the threat. Instead, cyber deterrence should rely on a 'campaign'. This closely mirrors a persistent engagement approach. However, unlike that approach, it has a holistic – rather than military – focus because it includes diplomatic, economic and informational options.[41]

KEY RECOMMENDATIONS

At this early stage of the project, the following, most pressing, recommendations have emerged. These form the foundations for a cumulative and tailored approach to deterring malicious cyber activity.

FRAME CYBER THREATS PRAGMATICALLY

First, policymakers and defence stakeholders should be cautious not to over-inflate the significance of a hypothetical 'big event' cyber incident. Zealous curiosity about unexpected critical service outages, such as for the 2025 Spain and Portugal power cut, can feed this tendency.[42] While there is a compelling 'fiction becoming reality' pull to such narratives,[43] they are not necessarily conducive to progressing a pragmatic approach to implementing cyber deterrence.

Second, policymakers might look at existing crisis response units (that is, those for natural catastrophes or 'traditional' kinetic effects) across agencies to understand correlation and/or learning opportunities for cyber and non-cyber preparedness, response and communication strategies. Doing so may allow them to better position economic, social and political impacts of cyber incidents within a more proportionate framing – and thus more appropriately

41. Persistent engagement can establish friction in cyberspace, signal capabilities to adversaries and even establish tacit understandings of acceptable/unacceptable operational behaviour, but not be a decisive credible deterrent to future activities. To deter in this way, cyber campaigns need to be carefully integrated into, and analysed as part of, a broader approach to deterrence. Also see James N Miller and Neal A Pollard, 'Persistent Engagement, Agreed Competition and Deterrence in Cyberspace', *Lawfare*, 30 April 2019, <https://www.lawfaremedia.org/article/persistent-engagement-agreed-competition-and-deterrence-cyberspace>, accessed 27 May 2025; and Jacquelyn G Schneider, 'Persistent Engagement: Foundation, Evolution and Evaluation of a Strategy', 10 May 2019, *Lawfare*, <https://www.lawfaremedia.org/article/persistent-engagement-foundation-evolution-and-evaluation-strategy>, accessed 27 May 2025.
42. Elini Kemene and Anne Christianson, 'What We Can Learn about Building a Resilient Energy Grid from the Iberian Power Outage', World Economic Forum, 16 May 2025, <https://www.weforum.org/stories/2025/05/resilient-energy-grid-iberian-power-outage/>, accessed 19 May 2025.
43. Gareth Mott, *Constructing the Cyberterrorist: Critical Reflections on the UK Case* (Abingdon: Routledge, 2019).

calibrate perceptions of impact and institutional responses to cyber incidents and their effects (intentional or not).[44] It may also highlight opportunities to integrate cyber effects with other disruptions in the grey zone.

Third, to frame cyber threats pragmatically and calibrate deterrence measures, policymakers should consider a more targeted and contextually sensitive approach to their actions. This includes devising actor-specific deterrence strategies in addition to existing broader national and regional frameworks. This 'tailored deterrence'[45] might allow for better calibration of cultural, regional and contextual factors that are detrimental to the impact, measurement and effectiveness of deterrence. Moreover, a context-sensitive approach might lead to better calibration of the 'shelf-life' or desired frequency of use of a deterrence mechanism (how much impact it can deliver and for how long).[46] While states may already engage in tailoring – both privately and publicly – this has limited 'signalling' impact if it is not disseminated on a clear and timely basis.

In the following stages of this research project, RUSI will work to support the pragmatic framing of cyber threats, with the specific objective of mapping these to a menu of deterrence options.

If states are serious about cyber deterrence, they need to understand the relationship between ... political will and geostrategic context

WORK TOWARDS AGREEMENT ON MEANINGFUL RED LINES IN CYBER EFFECTS

Judged by their scale, catastrophic cyber incidents are (at present) unlikely to reach the threshold of armed conflict. However, if states are serious about cyber deterrence, they need to understand the relationship between two elements that are arguably decisive: political will and geostrategic context. Generally, states will not frequently signal or invoke the crossing of a threshold due to cyber actions, but political will and geostrategic context might be the most critical factors in a decision to do so. For example, Costa Rica declared for the first time a state of emergency due to a cyber incident, but never officially and publicly said Conti was affiliated with Russia.[47] Albania, in contrast, was the first country to cut diplomatic ties (in this case with Iran) due to a cyberattack[48] – a much more politically relevant

44. It is important to note that it is often challenging to determine the intentionality of effects but, whenever possible, responses should be calibrated according to (but not exclusively) that variable.
45. Lantis, 'Strategic Culture and Tailored Deterrence'.
46. For example, naming and shaming might have an impact for another country's foreign policy if done for the first time. However, if used frequently, such impacts may diminish.
47. Kevin Collier, 'Costa Rica Declares State of Emergency over Ransomware Attack', *NBC News*, 11 May 2022, <https://www.nbcnews.com/tech/tech-news/costa-rica-declares-state-emergency-ransomware-attack-rcna28415>, accessed 1 August 2025.
48. Maggie Miller, 'Albania Weighed Invoking NATO's Article 5 over Iranian Cyberattack', *Politico*, 5 October 2022, <https://www.politico.com/

move for signalling unacceptable behaviour in inter-state relations and highly reflective of the rising tensions between the two countries. Another example is Iran's decision to attribute a 2019 cyberattack against one of its intelligence units to the US.[49] The decision to attribute was part of a broader context of rising tension between the US and Iran in the Strait of Hormuz, which again shows that context and political appetite matter. However, on their own, cyber operations in a context such as this have more in common with a strategy of escalation management than deterrence. This further endorses the need to rethink the role of cyber in deterrence more generally. The pairing of cyber as an escalation-management tool with kinetic or other economic and diplomatic means of deterrence[50] points to potential game-changing elements in deterring hybrid threats in the grey zone.

Like-minded Western states have articulated that a cyber operation might constitute an act of war,[51] but there is significant cultivated ambiguity on what the threshold is, and which actions would breach it. Interpretations of how international law applies to cyberspace are also growing but may still be insufficient to objectively shape customary international law. Such ambiguity is understandable, reflecting a pragmatic desire to avoid both unnecessary escalation and the tying of one's own hands. However, this also undermines the formation of clear signalling of the degree of cyber incursion that would (or could) constitute an act of war equivalent to a conventional strike.

Where political and contextual appetite for strong deterrence measures is uncertain, a lack of threshold demarcation significantly diminishes options for deterrence as well as their effectiveness. Like-minded Western states should consider how they can signal red lines with greater credibility, while maintaining the operational and strategic ambiguity required to consider incursions on a case-by-case basis. The authors recognise that ambiguity may, itself, have a deterrent effect and may be a strategic necessity to maintain contextual flexibility, including the flexibility to de-escalate. However, ambiguity can also have a dampening effect on a state's capacity to signal credibly.

Additionally, policymakers and strategists in like-minded Western states should consider whether it is possible and desirable to outline which actions would constitute a threatening of the use of force by cyber means.

---

news/2022/10/05/why-albania-chose-not-to-pull-the-nato-trigger-after-cyberattack-00060347>, accessed 14 July 2025.

49. *Reuters*, 'Iran Says it Dismantled a US Cyber Espionage Network', 17 June 2019, <https://www.reuters.com/article/world/iran-says-it-dismantled-a-us-cyber-espionage-network-idUSKCN1TI1IZ/>, accessed 4 August 2025.
50. Julian E Barnes, Eric Schmitt and Thomas Gibbons-Neff, 'White House is Pressing for Additional Option, Including Cyberattacks, to Deter Iran', *New York Times*, 20 May 2019.
51. James Pearson and Jonathan Landay, 'Cyberattack on NATO Could Trigger Collective Defence Clause – Official', *Reuters*, 28 February 2022.

For instance, pre-positioning in a particular critical system might, in some circumstances, constitute a threat of force and a violation of the UN Charter.[52]

BREAK INERTIA AND CONSIDER ALL OPTIONS

This paper has highlighted that there is a wide array of middle-ground cyber incursion activity that is sub-threshold. Nonetheless, such activity poses national security risks and societal harms. Policymakers and strategists should consider whether there are opportunities to signal intent and rapidly respond to incursions that currently would not receive a response or would have a delayed reaction months later. Understandably, rapid and firm reactions to middle-ground events may be difficult to coordinate quickly with allied states. Nonetheless, there may be opportunities to draw on a menu of options and take action to signal firmer red lines as part of a broader deterrence campaign.

Additionally, it should be noted that deterrence can require threatening something at least equivalent to, but ideally greater than, the threatened or actualised incursion. At the 2025 Paris Summit of the Pall Mall Process, a member of the US National Security Council raised the possibility of lethal force against adversarial actors involved in the commercial offensive cyber industry.[53] While the comment received consternation, lethal force is used in domestic and international operations against sub-threshold threats such as terrorism and piracy. Doubtless, a drone strike against the notorious cybercrime group Evil Corp in Russia would be logistically harder – and more hair-raising – than one against, for instance, Houthi militants in Yemen. However, consideration could be given as to when and how 'big sticks' or covert action could be used to enforce deterrence, even if the provoking incursion is sub-threshold.

CONCLUSION

Although expert views on cyber deterrence remain divided, with some rejecting the concept entirely, this paper advocates for the adoption of cross-domain deterrence to reduce hostile state-sponsored cyber activity. It draws on diplomatic and financial toolkits, among other levers. Rather than 'unrealised and unspecific scaremongering' that risk overshadowing the important shift in the threat picture[54] – stealthier, more sophisticated and large-scale pre-positioning by some actors – ongoing policy research and dialogue should draw from and advance the practical understanding of a cyber-oriented view of cross-domain deterrence.

52. Skingsley, 'Cyber-Rattling'.
53. Alexander Martin, 'As Spyware Market Continues to Expand, Diplomatic Pall Mall Process Hits a Pivot Point', *The Record*, 9 April 2025, <https://therecord.media/pall-mall-process-commercial-spyware-hacking-paris-diplomacy>, accessed 19 May 2025.
54. Martin, 'Typhoons in Cyberspace'.

Research findings also recognise the political appetite of major Western states to adopt more assertive measures in response to hostile activity in cyberspace.[55] Historically, cyber activity was often linked to espionage and intelligence activities, and thus considered beyond the scope of traditional deterrence strategies. Now, given the urgency to respond to existing geopolitical threats, the push for a new European defence and security architecture and recent examples of increasing political and strategic adversary activity in cyberspace, there is a vital and time-sensitive opportunity to assess the role of cyber in contemporary deterrence strategies.

A cross-domain approach should support the development of tailored and cumulative deterrence strategies. This approach, drawing on multiple levers in cyber and beyond, could support states in devising strategies that address specific actors – and can therefore be more carefully crafted in light of the adversary's strategic culture as well as assessed in terms of effectiveness and implementation with specific indicators – and reflect on effectiveness or gains against the adversary over time. Doing so could then lead to like-minded governments collaborating on actor-specific deterrence frameworks and more purposefully developing joint deterrence strategies. Such strategies would include cyber-specific interventions (that is, joint attributions, takedowns and/or cyber operations to deny, degrade and disrupt an adversary's capacity). However, in isolation, these will not be enough. Further RUSI research will assess the wider spectrum of interventions.

Taken together, this layered strategy might help to disincentivise some sub-threshold malicious cyber activity while also laying the groundwork for more forceful responses to severe incursions. To advance this agenda, two workstreams are proposed to work towards the goal of a common framework of cyber deterrence that is accessible for policymakers.

First, it would be helpful to build on the spectrum of cyber operations and impacts articulated in this paper to understand cumulative deterrence with a range of real and hypothetical case studies. Second, as this paper has highlighted, there are lessons to be shared across the multiple informal schools of thought on cyber deterrence. Stakeholders and experts with diverse perspectives on cyber deterrence need to be brought together and collaborate creatively with traditional deterrence strategists, thereby facilitating a more integrated and pragmatic framework. To this end, tailored research engagements will be used to bridge this gap – moving from the semantic and conceptual deadlock of 'cyber deterrence' to operational, actor-specific deterrence fit for today's threat environment.

55. Greg Otto, 'National Security Council Cyber Lead Wants to "Normalize" Offensive Operations', *CyberScoop*, 1 May 2025, <https://cyberscoop.com/alexei-bulazel-white-house-national-security-councial-destigmatize-offensive-cyber-rsac-2025/>, accessed 4 June 2024.

ABOUT THE AUTHORS

Louise Marie Hurel is a Research Fellow in RUSI's Cyber and Tech team, where her work focuses on cyber diplomacy, tech supply chain security, cyber attribution, cybersecurity companies' role in statecraft and cyber capacity building. Louise also leads RUSI's Partnership for Responsible Cyber Behaviour. Her doctoral research at the London School of Economics and Political Science (LSE) focuses on the history of private authority and the political economy of private companies in cybersecurity.

In addition to her research, Louise is a Senior Associate Fellow at both Virtual Routes and the Brazilian Centre for International Relations (CEBRI), co-chair of the Global Forum on Cyber Expertise (GFCE) Strategic Steering Committee, and an appointed member of Brazil's National Cybersecurity Committee. In 2023, Louise was nominated as a 35 under 35 Future Leaders by CIDOB-Santander.

Gareth Mott is a Research Fellow in the Cyber and Tech team at RUSI. His research interests include governance and cyberspace, the challenges (and promises) of peer-to-peer technologies, developments in the cyber risk landscape, and the evolution of cyber security strategies at micro and macro levels.

194 years of independent thinking on defence and security

The Royal United Services Institute (RUSI) is the world's oldest and the UK's leading defence and security think tank. Its mission is to inform, influence and enhance public debate on a safer and more stable world. RUSI is a research-led institute, producing independent, practical and innovative analysis to address today's complex challenges.

Since its foundation in 1831, RUSI has relied on its members to support its activities. Together with revenue from research, publications and conferences, RUSI has sustained its political independence for 194 years.

Royal United Services Institute
for Defence and Security Studies
Whitehall
London SW1A 2ET
United Kingdom
+44 (0)20 7747 2600
www.rusi.org

RUSI is a registered charity (No. 210639)