

Insights Papers

September 2026

# Beyond ‘Cyber’ in Deterrence: A Multilevel Framework

Louise Marie Hurel and Gareth Mott

RUSI

## Disclaimer

The content in this publication is provided for general information only. It is not intended to amount to advice on which you should rely. You must obtain professional or specialist advice before taking, or refraining from, any action based on the content in this publication.

The views expressed in this publication are those of the authors, and do not necessarily reflect the views of RUSI or any other institution.

To the fullest extent permitted by law, RUSI shall not be liable for any loss or damage of any nature whether foreseeable or unforeseeable (including, without limitation, in defamation) arising from or in connection with the reproduction, reliance on or use of the publication or any of the information contained in the publication by you or any third party. References to RUSI include its directors, trustees and employees.

© 2026 The Royal United Services Institute for Defence and Security Studies



This work is licensed under a Creative Commons Attribution – Non-Commercial – No-Derivatives 4.0 International Licence. For more information, see <http://creativecommons.org/licenses/by-nc-nd/4.0/>.

RUSI Insights Papers, September 2026

## Publications Team

**Editorial**

Director of Publications: Alice Trouncer

Managing Editor: Sarah Hudson

Assistant Editor: Sophie Boulter

Assistant Editor: Liz Ottosson

**Design**

Graphic Designer: Lisa Westthorp

**Research Editorial**

Head of Research Governance and Editorial: Elias Forneris

Cover image: Suriyo / Adobe Stock. Generated with AI

## Get in touch

www.rusi.org

enquiries@rusi.org

+44 (0)207 747 2600

The Royal United Services Institute for Defence and Security

61 Whitehall, London

SW1A 2ET

United Kingdom

## Follow us on

## Methodology

This paper is the outcome of data gathered in 16 semi-structured interviews conducted with current and former government representatives from NATO member states and EU institutions, two workshops (one held in New York and the other in Tallinn) with approximately 30 stakeholders from governmental and non-governmental backgrounds, and two briefings to governmental representatives working on issues of cyber deterrence across Europe. These sources provide the corpus of primary data collected throughout the lifecycle of this research. This was complemented by secondary data from scholarly literature on cyber deterrence, campaigning and cross-domain deterrence. One of the workshops and one of the briefings were dedicated to testing and validating the framework presented in the following sections. During these occasions, the authors presented different versions of the framework, tested it with representatives from Allied states, and collected feedback for further development.

© Royal United Services Institute

# Introduction

In September 2025, approximately 20 drones penetrated Polish airspace, resulting in airport closures in Warsaw. The event prompted Poland to invoke Article 4 of the North Atlantic Treaty,[1] calling for a consultation with member states in the event of a threat. Three months later, a coordinated cyberattack targeted multiple distributed energy sites across Poland. Russia's provocations are mounting and becoming increasingly sustained. There may have been over 140 documented drone incursions between 2024 and 2026.[2] These flew over aircraft carriers,[3] ports and airbases across Europe, and were compounded by influence campaigns,[4] subsea cable sabotage,[5] and cyberattacks. These examples highlight the cross-domain and increasingly integrated nature of hybrid threats in Europe.

Cyber-only responses (for example, attributions, cyber operations or cyber sanctions) to hostile state or state-tolerated cyber activity within broader hybrid campaigns are far from enough to constrain an adversary's strategic advantage across multiple domains. There is a lack of adequate multilevel, layered, coordinated and sustained action that uses all levers of government to combat malicious cyber activity. Achieving deterrence outcomes requires a whole-of-government effort. Cyber tools support that, but the other way around should also be true: slowing down, disrupting and/or denying malicious actors from achieving strategic advantage in and through cyberspace should benefit from a whole-of government approach. States across Europe are at risk of measuring effectiveness (or lack thereof) narrowly in cyber terms or focusing solely on building cyber resilience at a time when they face costs from the actions of less restrained adversaries operating across multiple domains.

The pursuit and defence of national interests in a context of hybrid threats will increasingly depend on how well European states integrate and coordinate different capabilities to achieve deterrence outcomes, including in and through cyberspace. (Examples include: slowing down, disrupting, denying or degrading an adversary's

1. Chancellery of the Prime Minister of Poland, 'Poland Moves to Invoke NATO Article 4 After Airspace Violation', 10 September 2025, <https://www.gov.pl/web/primeminister/poland-moves-to-invoke-nato-article-4-after-airspace-violation>, accessed 10 June 2026.
2. Charlie Edwards, Rex Fox O'Loughlin and Louis Bearn, 'Russia's UAV Campaign over Europe', Research Paper, International Institute for Strategic Studies, June 2026, <https://www.iiss.org/research-paper/2026/06/russias-uav-campaign-over-europe/>, accessed 4 July 2026.
3. Dzirhan Mahadzir, 'Swedish Forces Jam Suspected Russian Drone Near French Carrier *Charles de Gaulle*', USNI News, 27 February 2026, <https://news.usni.org/2026/02/27/swedish-forces-jam-suspected-russian-drone-near-french-carrier-charles-de-gaulle>, accessed 4 July 2026.
4. Alden Wahlstrom and David Mainor, 'Pro-Russia Information Operations Leverage Russian Drone Incursions into Polish Airspace', Google Cloud Threat Intelligence Blog, 21 October 2025, <https://cloud.google.com/blog/topics/threat-intelligence/pro-russia-information-operations-drone-incursions>, 4 July 2026.
5. *Recorded Future*, 'Submarine Cables Face Increasing Threats Amid Geopolitical Tensions and Limited Repair Capacity', 17 July 2025, <https://www.recordedfuture.com/research/submarine-cables-face-increasing-threats>, accessed 5 July 2026.

© Royal United Services Institute

capacity to act in and through cyberspace; and managing and/or changing the behaviour of middle-ground states.) States therefore need to domestically assess the multidomain capabilities at their disposal and evaluate the concrete versus expected added value of such capabilities in the context of traditional and non-traditional threats, such as cyber activity.

There has been some progress, including: legislative adaptations[6] to enable proactive responses to cyber threats;[7] EU efforts to increase the frequency of cyber sanctions; and the establishment of broad coalitions of states that support cyber attributions. However, the speed of responses is far from consistent, and the responses themselves are often confined to cyber-only bodies[8] and matters, and have only a limited focus on constraining adversarial activity.

Analytically, academic and policy research has primarily focused on the assessment individual tools.[9] **This paper argues for a whole-of-government approach to achieving the deterrence outcome[10] of degrading, disrupting, denying and constraining adversaries from gaining strategic advantage in or through cyberspace.** The framework and approach in this paper complement earlier efforts, but it treats the combination of instruments/tools as the primary unit of analysis. **It presents a**

6. Daryna Antoniuk, 'Dutch Government Passes Law to Criminalize Cyber-Espionage', *The Record*, 20 May 2025, <https://therecord.media/netherlands-law-criminalizes-cyber-espionage>, accessed 5 July 2026; Sven Herpig, 'Germany's New Cyber Active Defense Law', *Interface*, 18 March 2026, <https://www.interface-eu.org/publications/written-statement-on-germanys-new-active-cyber-defense-law>, accessed 4 July 2026; Markus Wacket, 'Germany Seeks Powers for Spies to Hack, Disrupt Attackers', *Reuters*, 2 July 2026.
7. Jason Blessing, 'The Global Spread of Cyber Forces, 2000–2018', paper presented to the 13th International Conference on Cyber Conflict, Tallinn, May 2021, <https://ccdcoe.org/uploads/2021/05/CyCon_2021_Blessing.pdf>, accessed 1 August 2026; Matthias Schulze, 'How European and Allied Cybersecurity Strategies Are Shifting from Defence to Offence', *Binding Hook*, 27 January 2026, <https://bindinghook.com/how-european-and-allied-cybersecurity-strategies-are-shifting-from-defence-to-offence/>, accessed 15 June 2026; Louise Marie Hurel, 'The Risk of Making Offensive Cyber the New Shiny Silver Bullet', EU Cyber Direct blog, 14 April 2026, <https://eucyberdirect.eu/blog/the-risk-of-making-offensive-cyber-the-new-shiny-silver-bullet>, accessed 15 June 2026.
8. Information provided by workshop participants, 27 May 2026; author interview, 3 December 2025.
9. Jiyoun Park and Boram Shin, 'Conceptualizing Digital Sanctions as a New Type of Economic Sanctions in the Digital Era: Digital-Related Sanctions Measures Against Russia and Their Consequences', *Journal of Eurasian Studies* (Vol. 16, No. 1, 2025), pp. 44–59; Jason Healey, Neil Jenkins and J D Work, 'Defenders Disrupting Adversaries: Framework, Dataset, and Case Studies of Disruptive Counter-Cyber Operations', paper presented to the 12th International Conference on Cyber Conflict, Tallinn, May 2020, <https://ccdcoe.org/uploads/2020/05/CyCon_2020_14_Healey_Jenkins_Work.pdf>, accessed 10 June 2026; Michael P Fischerkeller and Richard J Harknett, 'Persistent Engagement and Cost Imposition: Distinguishing Between Cause and Effect', *Lawfare*, 6 February 2020, <https://www.lawfaremedia.org/article/persistent-engagement-and-cost-imposition-distinguishing-between-cause-and-effect>, accessed 20 August 2026; Florian J Egloff and Max Smeets, 'Publicly Attributing Cyber Attacks: A Framework', *Journal of Strategic Studies* (Vol. 46, No. 3, 2023), pp. 502–33.
10. Other scholars have argued that cyber campaigns are key means through which states might achieve, over time, cumulative outcomes that lead to strategic advantage. This paper refers to broader actions, including non-cyber, that can support broader campaigning (pending resources, political commitment, and capacity, among others) to achieve such cumulative outcomes and strategic advantage in and through cyberspace. On the former, see Richard J Harknett and Max Smeets, 'Cyber Campaigns and Strategic Outcomes', *Journal of Strategic Studies* (Vol. 45, No. 4, 2022), pp. 534–67.

© Royal United Services Institute

**framework for multilevel responses that integrate cyber tools – such as offensive cyber capabilities – with other non-cyber tools that can support states across NATO in achieving deterrence outcomes.** Previous RUSI research has already argued for a cross-domain and multilevel (beyond domains) approach where cyber is part of a portfolio of threatened response options.[11] This paper introduces how other levers of government (that is, diplomatic, economic or military) should be employed and how they may be more effective than a cyber-only approach to slowing down malicious cyber activity.

The paper first introduces the framework for multilevel action against malicious cyber activities along with its four key functions: raising the bar; imposing costs; benefits and inducements; and enablers that strengthen the previous three functions. The framework presented in the following sections is a condensed view of the 52 tools we have identified across these four functions. The full framework is available as a separate and interactive resource at https://www.rusi.org/explore-our-research/publications/insights-papers/beyond-cyber-deterrence-multilevel-framework. The framework should be seen not as an exhaustive account, but as a practical instrument for government representatives.

Next, the paper operationalises the framework, providing two pathways for states to use existing cyber and non-cyber tools for national security. One pathway is **multitool calibration according to behaviour**: the intensity and the tools used are indexed to an assessment of observed behaviour from the other state. The other pathway refers to **layering of costs and multitool sequencing**: tools are leveraged to have a compounding effect over an adversary over time, each creating the conditions for the use of the next one.

The framework is intended to support NATO/EU member states and Allies in at least three ways. The first way is triggering or informing existing domestic cross-departmental assessments for areas where cyber and non-cyber tools are already in use, and how to best coordinate their use and expansion. The second is illustrating how multilevel action can be used against adversaries. The third is demonstrating how these actions need to be thought about and operationalised. Doing so is as important for managing relationships with third countries as with adversaries, if they are to produce cyber deterrence outcomes in a sustained fashion.

11. Louise Marie Hurel and Gareth Mott, 'Rethinking Cyber Deterrence in a Multipolar World', *RUSI Emerging Insights*, August 2025, <https://www.rusi.org/explore-our-research/publications/emerging-insights/rethinking-cyber-deterrence-multipolar-world>, accessed 13 June 2026.

© Royal United Services Institute

In this paper**, 'cyber deterrence' refers to the outcomes that can be achieved through sustained, cumulative, grey-zone oriented, iterative, tailored and cross-domain activities and effects to slow, degrade, disrupt and deny malicious cyber activity**.[12] The paper is concerned with the deterrence of malicious cyber activity, not with a narrow reading of deterrence as singularly delivered through (albeit supported by) cyber means. Cyber instruments do appear throughout the framework, and some of them contribute to deterring outcomes in other domains. However, the object deterred here is cyber activity.

# Framework

This section presents the framework that the authors developed and tested through workshops and briefings. It reflects what interviewees made clear: European states need more accessible language to describe the activities Allies undertake and the effects they seek to achieve. The non-exhaustive framework encompasses actions that might be taken not only against an adversary but also for the management of relationships and behaviours from third countries (neither Allies nor adversaries). The purpose of the framework is to provide NATO and EU policymakers and operators with a shared analytical framework to achieve at least three objectives.

The first objective is to situate cyber tools within a broader toolset, with the aim of supporting governments in identifying which tools are appropriate and which conversations (inter-departmental or ministerial) are necessary to integrate cyber and non-cyber tools for cyber deterrence outcomes.

Second, the framework enables practitioners in specialised departments (for example, cyber commands, ministries of foreign affairs and ministries of defence), or those performing cyber-related functions, to use existing tools more purposefully with the aim of translating existing non-cyber tools for whole-of-government efforts to curb malicious cyber activity.

Third, the framework aids understanding of how those tools relate to, sequence with, and reinforce one another in achieving deterrence outcomes. Such an approach enables an outcomes-driven toolkit selection that is based in whole-of-government action rather than a toolkit-driven discussion where each tool's value is assessed in isolation.

The framework focuses on four key tool functions, described below. The framework focuses on what a tool does (or promises to do) to an adversary's cost-benefit analysis of conducting malicious cyber operations rather than who owns it. Ownership may vary across institutional setups in the Alliance and across European capitals.

12. A more detailed explanation of this definition of deterrence, and of its variables, is set out in Hurel and Mott, 'Rethinking Cyber Deterrence in a Multipolar World'.

© Royal United Services Institute

## Four Functions

The framework presents tools in four non-exhaustive functional categories. Figure 1 provides a visual representation of cyber and non-cyber tools used to achieve cyber deterrence outcomes across all four categories. These categories are:

- **Raising the bar:** Actions and instruments that reduce the likelihood, impact and/or payoff of malicious cyber operations by making attacks and operations harder to conduct, politically and/or technically costlier to attempt and less rewarding when executed.
- **Imposing costs:** Actions and instruments that actively degrade, disrupt, slow down and impose consequences on adversaries or third countries conducting and/or harbouring malicious cyber activity, through periodic or persistent proactive activity and/or reactive punishment.
- **Benefits/inducements:** Positive measures such as rewards or withdrawal of penalties based on conditionalities that are offered to adversaries, perpetrators, harbouring states or negligent states in exchange for – or as a recognition of – restraint and/or behavioural change. The framework covers two types of benefits: rewards (for example, market access and technology cooperation/exchange); and penalty relief (for example, lifting of sanctions and removal from grey lists).
- **Enablers:** Cross-cutting foundational instruments that do not stop malicious cyber activity but strengthen the effectiveness of both raising the bar and imposing costs (for example, attribution capacity, capacity building and public–private cooperation).

© Royal United Services Institute

**Figure 1:** Condensed View of Tools Enabling Cyber Deterrence Outcomes

| | | Raising the Bar | Imposing Costs (Proactive Posture) | Benefits/Inducements | Enablers |
|---|---|---|---|---|---|
| **Cyber Tools** | | • Security standards and hardening<br>• Active cyber defence<br>• Vulnerability detection, management and mitigation | • Offensive cyber operations/ campaigns<br>• Defence forward (unilateral)<br>• Hunt-forward operations (joint)<br>• Seizure/disruption of infrastructure | • Inclusion/belonging to a trusted defence community<br>• Preferential or privileged access to threat intelligence | • Capacity to attribute<br>• Access to licences and adequate tech tools<br>• Public–private cooperation (JCDC, DCU)<br>• Threat intelligence-sharing partnerships<br>• Capacity building<br>• Strong development institutions and funding avenues<br>• Espionage / persistent access (foundational)<br>• Alliance frameworks (for example, NATO Article 5)<br>• Joint commitments (for example, NATO Defence Pledge)<br>• Intelligence-sharing framework in place |
| **Non-Cyber Tools** | **Economic** | • Export controls<br>• Supply chain security<br>• Digital trade frameworks | • Targeted sanctions<br>• Financial disruptions (crypto, anti-money laundering)<br>• Tariffs and trade conditionalities | • Sanctions relief in response to adequate restraint<br>• Restoring or enabling market access (new agreements<br>• Tech cooperation / investments | |
| | **Diplomatic/ Legal** | • International cyber norms<br>• International law<br>• Confidence-building measures<br>• Moratorium and restraint pledges | • Public attribution<br>• Indictments<br>• Diplomatic expulsions<br>• Démarches | • Potential avenues for bilateral cooperation and MOUs in areas of convergence<br>• Coalition building at the multilateral, regional or 'likeminded' levels | |
| | **Counter-terrorism/ Arms control** | • Non-proliferation frameworks for cyber tools | • Safe-haven denial | • Removal from grey list or designation with conditionalities based on compliance | |
| | **Military** | • Well-established partnerships and/or alliance commitments<br>• Periodic military exercises in place | • Threat of physical strikes against cyber infrastructure<br>• Cyber supporting military operation | • Security guarantees through military alliances and partnerships<br>• Defensive (and offensive?) capability transfers (personnel, technology, knowhow, processes) | |
| | **Intelligence** | • Counterintelligence as a protective measure of own assets | • Covert action against adversary operations, campaigns and programmes<br>• Intelligence declassification and/or disclosure as exposure<br>• Recruitment degradation | • Intelligence-sharing access as a reward for alignment | |
| | **Cognitive/ Informational** | • Media literacy and counter-disinformation<br>• National agency/agencies dedicated to societal informational resilience and/ or exposing campaigns<br>• Clear models for communicating with domestic audiences | • 'Cognitive effects' on adversaries and decision-makers<br>• PsyOps targeting operators<br>• Sustained narrative campaigns<br>• Exposing influence campaigns | • N/A | |
| | **Development** | • Structured and targeted cyber capacity building (CCB) programmes | • Imposing conditionalities on assistance/CCB<br>• Severing contracts if commitments are broken | • Opportunity for expanded CCB for compliant partners<br>• Access to concessional digital development finance | |

Source: The authors.

© Royal United Services Institute

## Interdependence of Tools

These interdependent tools may be used against a competitor state to encourage (or force) behavioural change and/or to constrain its opportunities for strategic advantage in cyberspace. They may also be used against other states (not necessarily adversaries) to manage relationships with the aim of achieving deterrence outcomes.

A whole-of-government approach to achieving cyber deterrence outcomes enables the centralised coordination and review of tools. Analytically, it shifts the debate from a siloed approach where each department is trying to articulate the value of the tools it 'owns' to an outcomes-driven strategy. This fosters greater awareness and acknowledgement of tools and the mapping and modelling of their relationships and interdependencies, and provides the space for calibrating a mix of raising the bar, imposing costs, enablers and inducements to manage relationships and potential outcomes.

In some instances, one tool may be a prerequisite for another. In other instances, a tool may be used to amplify another. It is also possible that some tools may hinder the use of others or make them less effective, depending on the objective.

The interviews conducted for this paper emphasised the need for a coordinated approach. For example, one practitioner described how 'it is hard to say what the most effective tools are. We need to use a variety of them, maybe it is the compounded approach … it is a combination, to have a sustained long-term approach using all the tools available'.[13] A practitioner noted that cyber tools could 'amplify' or 'enable' other deterrence levers.[14] Another stressed that although the UK had an integrated approach with 'activities across the toolbox', there was a need to increase coordination between departments.[15] A practitioner gave an example of coordination, describing a scenario in which the Foreign, Commonwealth & Development Office collaborate with the National Cyber Security Centre as part of a sanctions package against Russian GRU units.[16] They emphasised that this also became a latch for international coalition activity with NATO, EU and partner countries, resulting in 30 national supporting statements. The interviewee described this as a 'first step' and highlighted the UK's ambition to do more coalition building. Seen in this light, an attribution and sanctions package might be both a prerequisite and an amplifying push for later use of tools on a collaborative basis.

13. Author interview, 17 December 2025.
14. Author interview, 27 November 2025.
15. Author interview, 6 November 2025.
16. Author interview, 6 November 2025; HM Government, 'Profile: GRU Cyber and Hybrid Threat Operations', 13 July 2026, <https://www.gov.uk/government/publications/profile-gru-cyber-and-hybrid-threat-operations/profile-gru-cyber-and-hybrid-threat-operations>, accessed 15 July 2026.

© Royal United Services Institute

This was a recurring finding throughout the research. Many interviewees described a need to develop and improve coordination between partner countries, particularly for cyber diplomacy tools where collective state action may carry greater weight than one country using a tool (for example, attributions) alone.[17]

As noted, some tools may hinder the use of others, or their objectives may conflict. For instance, an ongoing offensive cyber access-holding operation against an adversary's secure internal communication infrastructure may enable gathering of intelligence. In turn, this may guide strategic decision-making and, where possible, assessments of whether cyber deterrence outcomes are being achieved. It may also enable the delivery of an offensive cyber disruptive payload. But these two objectives may conflict: using the payload might sever the access.

Research participants consulted for this paper also described how Allies were binding their own hands needlessly – effectively 'deterring ourselves'.[18] They cited two factors. First, they said that Western governments were overestimating the likelihood of adversarial governments disproportionately responding to offensive cyber activity. Second, they said that cohesive tools – such as EU collective diplomatic and sanctions mechanisms – that require unanimous consent are underused because of the challenge of attaining that unanimity. For some EU member states, this may create a bind of reticence: they may be unwilling or unable to 'go it alone' but also unable to use the collective EU tools in an expedited way.

The framework is a template that governments can use, further populate, tailor and tweak to facilitate internal dialogue, map equities and identify areas that would benefit from further intervention to enable a coordinated whole-of-government approach.

## Cyber Deterrence Outcomes

This paper's framework calls for using cyber persistence,[19] defence, resilience and additional proactive measures as part of an integrated approach. The aim is to produce a deterring outcome in and through cyberspace. It is a multilevel integrated national security strategy for the digital age rather than a deterrence strategy (an aspiration). It does not assume a static and blanket approach to deterrence. Rather, it outlines potential outcomes that need to be achieved in and through cyberspace. It is urgent to move beyond cyber deterrence as strategy and reconceive it as an outcome: an objective that requires the full range of statecraft tools.

17. Author interview, 6 November 2025; author interview, 27 November 2025; author interview, 17 December 2025.
18. Information provided by workshop participants, 27 May 2026.
19. Michael P Fischerkeller, Emily O Goldman and Richard J Harknett, *Cyber Persistence Theory: Redefining National Security in Cyberspace* (New York, NY: Oxford University Press, 2022).

© Royal United Services Institute

Cyber deterrence outcomes refer to cumulative, iterative, partial and – in some cases – reversible changes in behaviour or activity of another state whether that is an adversary and/or third country. These outcomes need not be achieved using cyber-specific tools. Even though it is usually difficult to establish a causal link between tools and outcomes, states need to nonetheless be empowered to coordinate and use these resources with the aim of constraining adversaries in a more efficient and multilevel manner.

Accordingly, these outcomes also account for continual actions to raise the bar and enable tools. This means that, for example, an attribution campaign might not achieve the deterrence outcome of changing the behaviour of an adversary on its own. However, it may have enabled countries participating in the campaign to enhance their capacity to attribute, regardless of whether it is public.

Figure 2 outlines certain outcomes that are addressed in this paper. They are not exhaustive nor monocausal. Multiple indicators should be considered and triangulated over time to understand whether desired compounding effects are leading to deterrence outcomes.

**Figure 2:** Cyber Deterrence Outcomes and Indicative Observables

| Outcome | What Success Might Look Like | Indicative Observables |
|---|---|---|
| **Threshold compliance** | Assuming there is a clear threshold. Activity that the state declared as unacceptable does not occur, even when other kinds of activities continue. | Declared red lines communicated; target sets are avoided. |
| **Higher adversary cost per operation** | The adversary spends more time, money, personnel and talent per operation, campaign or mobilisation for cyber or non-cyber activity. | Change in re-tooling time after exposure or takedown; re-acquisition or reconstruction time for infrastructure; change in tactics, techniques and procedures. |
| **Escalation control** | The adversary self-censors activities below thresholds. | Behaviour during crisis periods; pre-emptively using private channels of communication to deconflict or clarify intent of non-malicious effect. |
| **Denial of strategic advantage** | Access gained by the adversary does not convert into coercive leverage or operational effect. The partner country actively rejects harbouring or addresses negligent behaviour, thus hindering adversarial use of infrastructure in other jurisdictions. | Pre-positioning discovered and access revoked before use. The partner country cooperates in the disruption of adversarial activity. |
| **Third-party behavioural change** | Complacent, unable (lacking capacity) or harbouring states cooperate, rather than tolerating malicious cyber activity. | Willingness to co-sign or discuss attributions; reduction of hosting of malicious infrastructure or activity; cooperation on hunt-forward-like operations or law enforcement takedowns requests. |
| **Restored or enhanced freedom of action** | Allies are willing and able to use the tools they already have; lowering of self-deterrence across European capitals. | Reduction in time to respond to incidents (whenever responses with a shorter timeframe are desirable); number of states joining coalition statements or soft endorsements. |

Source: The authors.

© Royal United Services Institute

# Operationalising the Framework: A Multi-Action Strategy

Governments face a challenging, but nonetheless vital, task of operationalising this framework. There are visible costs of operationalising a layered and multilevel approach to achieving deterrence outcomes in government. When budget lines are tight, the difficult-to-calculate and diffuse cost of absorbing hostile activity makes it especially challenging for governments to justify institutional changes and investments. This means that there is a risk that advocates of a whole-of-government approach become stuck in cycles of policy attention that are driven by episodic cases but occur within a context where adversarial activity should be considered as a multilevel constant. The wider context demands an equally sustained and campaigns-based effort.

There are at least four alternatives to the multilevel approach. Currently, these are presented as piecemeal approaches that do not reflect a multidomain action from adversaries: focus on resilience and defence alone; cyber-only responses; episodic or one-off responses to sustained adversarial action; and sustained strategic ambiguity in response.

Instead, the next sections demonstrate how states can operationalise a whole-of-government approach with existing tools. They build on recommendations raised by participants throughout the interviews, workshops and briefings. Albeit not exhaustive, they indicate areas for intervention and refinement of cyber and non-cyber tools to achieve cyber deterrence outcomes. These can help states to design strategies for raising the bar, imposing costs, creating positive inducements and strengthening enablers.

Future research[20] will also look more closely at how an individual state can avoid the need to develop every multilevel tool, and draw on collective strengths. This can be achieved through a combination of collective action and an awareness of complementary capabilities across Europe.

## Calibrating Responses to Behaviour

### Refining Cyber Tools for 'Proactive' Partnerships

Certain instruments in the framework do more than impose costs and raise the bar; they build relationships that can further enable both. That is the case, as noted by interviewees and project participants, of hunt-forward operations (HFOs). These operations were first doctrinally conceived and communicated by the US Cyber

20. RUSI, 'State Responsibility and Cyber Deterrence', <https://www.rusi.org/explore-our-research/projects/state-responsibility-and-cyber-deterrence>, accessed 10 August 2026.

© Royal United Services Institute

Command and play into its posture of persistent engagement. Teams will not only focus on defending networks and 'waiting for an intrusion to be identified', but also proactively[21] hunt for adversary malware within local networks and beyond. HFOs refer to those operations where a state deploys teams to a partner's networks at its request to identify and expose adversaries' activities. According to the US Cyber Command, '[t]he findings of HFOs, as well as other USCYBERCOM operations, are then shared with the public',[22] although the sensitivities surrounding these operations mean that primary partners, affected parties or compromised vendors might access the information – but few details of the vulnerabilities are made public. The UK has also been reportedly[23] conducting similar operations although it has been less vocal about where they have taken place and which partners were involved. Other models[24] have also been devised across Europe. These have a greater focus[25] on response and recovery from incidents, rather than proactive bilateral partnership to hunt for adversarial activity across jurisdictions – as far as has been publicly reported.

While not all states will replicate the US approach to HFOs – which, according to US Cyber Commander General Joshua Rudd, has amounted to over 100 deployments in over 30 countries[26] in recent years – others can still benefit from the model by working on foundational elements. These include: developing the right enablers such as host-nation consent frameworks;[27] assigning dedicated support teams to work with the host nation in a sustained fashion; establishing intelligence and operational frameworks to enable coordination; and creating a list of regions and/or countries that should be prioritised for such trust-building activities.

21. Paul M Nakasone and Michael Sulmeyer, 'How to Compete in Cyberspace: Cyber Command's New Approach', *Foreign Affairs*, 25 August 2020.
22. 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 1 July 2026
23. Alexander Martin, 'British Army General Says UK Now Conducting "Hunt Forward" Operations', *The Record*, 25 September 2023, <https://therecord.media/uk-hunt-forward-operations-lt-gen-tom-copinger-symes>, accessed 2 July 2026.
24. Taylor Grossman, 'Cyber Rapid Response Teams', Cyber Reports No. 11, Center for Security Studies, ETH Zurich, November 2023, <https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2023-11-Cyber-Rapid-Response-Teams.pdf>, accessed 1 July 2026.
25. Permanent Structured Cooperation (PESCO), 'PESCO's Cyber Rapid Response Teams Support Safeguarding Moldova's Elections and EU Referendum', <https://www.pesco.europa.eu/pressmedia/pescos-cyber-rapid-response-teams-support-safeguarding-moldovas-elections-and-eu-referendum/>, accessed 1 July 2026.
26. Joshua M Rudd, 'Posture Statement of General Joshua M. Rudd, USA Commander, United States Cyber Command before the 119th Congress Senate Committee on Armed Services', 28 April 2026, <https://www.armed-services.senate.gov/imo/media/doc/rudd_opening_statement1.pdf>, accessed 14 June 2026.
27. Tacita McCoy-Parkhill, 'Integrating Hunt Forward Operations for Enhanced UK Cyber Campaigning', RUSI Cyber Effects Perspectives, 9 April 2026, <https://www.rusi.org/explore-our-research/publications/cyber-effects-perspectives/integrating-hunt-forward-operations-enhanced-uk-cyber-campaigning>, accessed 2 June 2026.

© Royal United Services Institute

Participants consulted for this study suggested that HFOs are still largely underused for enabling deterrence outcomes. They highlighted that HFOs can be useful for countries seeking to forge new partnerships at the operational and intelligence-sharing levels. That, in turn, may be helpful both for smaller coalition-building efforts within existing like-minded states – for example, the Netherlands's ambitions to forge a European Five-Eyes alliance[28] – and partnership building with regions and countries beyond Europe.[29]

The relationship-building character of HFOs makes them a potential tool for reaching out beyond the usual circle of allies. Operational cooperation can be extended to states that sit outside Alliance structures but are exposed to the same adversaries. The establishment of the structures and processes within and between supporter and partner/host country are critical enablers that can create new partnerships (and, therefore, pathways) for achieving deterrence outcomes. Additionally, HFOs support deterrence outcomes by raising the bar of the partner country – by hardening their systems as part of the defensive operation, and/or by the transfer and sharing of knowledge and skills during the collaboration. The supporting country also benefits from HFOs. The experience enables them to better understand how to tailor requirements and agreements to specific regions and contexts. Moreover, it also raises the bar due to their improved visibility of adversarial activities, tactics, techniques, procedures and – potentially – operational objectives in other regions. In turn, this allows for better operational planning, enhanced defence and a concrete contribution of cyber threat intelligence to broader intelligence gathering and profiling of a particular state threat.

Secondary benefits of HFOs may also involve signalling effects (political or operational) to adversaries and proxies, or to domestic audiences. Since 2022, the US has been more vocal in publishing press releases on HFOs that it had conducted, often naming the partner.[30] As with political public cyber attributions, public communications on HFOs do not solely result in deterrence outcomes or behavioural change. However, depending on the appetite of the country for tailoring HFO-like instruments to its deterrence toolbox, these can politically signal – to domestic audiences – the importance and role of public institutions in 'proactively' defending the country's networks by stopping malicious cyber activity 'at the origin'. Such instruments also have a role in signalling to the adversary. During one of the workshops, a participant noted both that HFOs were a trust-building exercise and that enhanced trust itself penalised (or facilitated penalties for) adversaries because such countries 'don't want

28. Government of the Netherlands, 'A Secure Netherlands and a Strong Society', 23 February 2026, <https://www.government.nl/government/coalition-agreement/a-secure-netherlands-and-a-strong-society>, accessed 2 July 2026.
29. Information provided by workshop participants, 27 May 2026; author interview, 2 February 2026.
30. Martin Matishak, 'US Cyber Command Conducted First Zambia "Hunt Forward" Mission Last Year', *The Record*, 21 May 2024, <https://therecord.media/us-cyber-command-hunt-forward-zambia>, accessed 5 July 2026.

© Royal United Services Institute

us to trust each other'.[31] Operational signalling might also be possible, whereby disruptions and mitigations in HFOs can indicate to the adversary a proactive and enhanced denial of access in, for example, the systems of a nation where they might have underestimated its capability to defend itself.

## Enhancing the Use of Economic Tools for Cyber

Economic coercion and deterrence have, in the past few years, become a recognisable feature of international disputes. States have shown growing willingness to deploy reciprocal and unilateral tariffs, to condition market access on behaviour, and to treat trade and investment as instruments of statecraft rather than as domains insulated from it. This normalisation of economic pressure creates an opening for cyber deterrence. The instruments that impose cost in a trade dispute can, in principle, be reoriented to enhance the costs for conducting malicious cyber activity. This section reflects on those tools that have been used and others that might be used for such purposes. It is also a reflection of consistent acknowledgements and interviewees' advocacy for the use of economic coercion for cyber, based on relationships (Allies, third-countries and adversaries) and behaviours.

Some of these tools such as sanctions, asset freezes, crypto wallet and exchange designations have already been used to disrupt and slow down malicious cyber actors. Examples of adaptation of some of these tools for cyber include the EU's Cyber Diplomacy Toolbox, established in 2017. This provides a framework within which member states can apply a horizontal cyber sanctions regime.[32] These measures sit alongside a separate Council of the European Union framework that targets Russia's destabilising hybrid activities abroad.[33] Both regimes can be used against the same actor. The challenge so far – as identified during the interviews[34] – is getting member states with varying degrees of maturity and perceptions of threats to converge on specific actions beyond Russia. Other tools, such as vendor-exclusion practices, have become increasingly notorious in the past five to seven years, but are mostly used as a retaliatory tool for concerns over compromised supply chains. That is the case for the EU's 2020 5G Cybersecurity Toolbox voluntary framework,[35] and the 2026 proposal of the EU Cybersecurity Act 2, which foresees[36] mandatory 'derisking' of European telecommunications operators from high-risk third-country suppliers.

31. Information provided by workshop participant, 27 May 2026.
32. Council of the European Union, 'Sanctions against Cyber-Attacks', <https://www.consilium.europa.eu/en/policies/sanctions-against-cyber-attacks/>, accessed 22 July 2026.
33. Council of the European Union, 'Russia's Hybrid Activities: EU Sanctions', <https://www.consilium.europa.eu/en/policies/sanctions-against-russia-hybrid-threats/>, accessed 22 July 2026.
34. Author interview, 10 November 2025; author interview, 20 February 2026.
35. European Commission, 'Secure 5G Networks: Commission Endorses EU Toolbox and Sets Out Next Steps', 29 January 2020, <https://ec.europa.eu/commission/presscorner/detail/en/ip_20_123>, accessed 22 June 2026.
36. European Commission, 'Commission Strengthens EU Cybersecurity Resilience and Capabilities', 20 January 2026, <https://ec.europa.eu/commission/presscorner/detail/en/ip_26_105>, accessed 22 June 2026.

© Royal United Services Institute

Economic tools, as seen in Figure 3, can be understood in a spectrum that is calibrated to a partner's or adversary's behaviour. These tools range from inducement to comprehensive isolation. The figure is illustrative of how states might want to plan the use of these cyber and non-cyber tools as behaviour and the relationship with the other state changes.

**Figure 3:** Tools Supporting Cyber Deterrence

**De-escalation: the gradient is reversible – verified improvement moves the relationship back up at every tier**

| | Harmonious | Drift | Material Concern | Serious Breach | Rupture |
|---|---|---|---|---|---|
| **Observed Behaviour** (the input) | Cooperates in good faith; aligns on norms; no malicious activity from territory and/or cooperation on shared threats | Ambiguous signals; low-level activity tolerance and identification; uneven due diligence due to lack of capacity | Persistent tolerance; clear activity originating from territory; unwillingness to remediate | Active harbouring or sponsorship; complicity; disruption of essential services; abandonment of commitments; remediation refusal | Sustained operations at or approaching use-of-force threshold; hostile alignment; persistent disruption of critical national infrastructure; sustained harbouring; little-to-no prospect of cooperation/ remediation |
| **Calibrated Measure** (the response) CARROT → STICK | **Inducements** Market access; preferential trade and investment agreements; offering of sanctions relief as positive inducement on de-escalation | **Financial Friction** Enhanced AML/ countering the financing of terrorism scrutiny; informal signalling; talks on existing activity and indicating potential remediation together | **Targeted Designations** Démarches; sanctions (threat of) on named actors and entities; threat of sectoral measures; crypto wallet and exchange designations | **Broad / Sectoral Measures** Sectoral sanctions; tariffs; export and technology controls; market-access conditionality tied to behaviours | **Comprehensive Isolation** Procurement and investment exclusion; scaling pressures through cumulative use of previous tools (for example, additional asset freezes); anti-coercion instruments |
| **Relationship Status** (the consequence) | FULL PARTNER | UNDER REVIEW | CONDITIONAL | SUSPENDED | SEVERED |

Source: The authors.

Figure 3 shows how responses might be calibrated and escalated as behaviour and/or the relationship with a state deteriorates. The EU's Anti-Coercion Instrument,[37] adopted in 2023 and often described in the field as the 'trade bazooka', is in the highest tier. The instrument is a standing authority to restrict market access, procurement and investment in response to economic coercion. It has never been activated; its value lies in the credibility of the threat rather than its use. The sequencing of tools illustrated above is merely indicative of how tools in the economic toolbox can be distributed according to behaviours. However, both the use and sequencing depend on a state's tolerance and perceived red lines.

37. European Parliament, 'EU Anti-Coercion Instrument: What Exactly is the "Bazooka"?', 20 September 2023, <https://www.europarl.europa.eu/topics/en/article/20230915STO05214/eu-anti-coercion-instrument-what-exactly-is-the-bazooka>, accessed 22 June 2026.

© Royal United Services Institute

There are two approaches in thinking about existing and new avenues for cyber/non-cyber complementarity of tools.

The first approach involves adapting existing economic instruments to cyber ends, as described above with the EU's establishment of a cyber sanctions regime. This transposition can be further enhanced by widening the scale and scope of the application of existing measures, such as expanding targeted sanctions and financial-disruption measures – moving from individual organisations to a series of organisations or to a sector.

The second approach involves building or adapting existing economic mechanisms for cyber deterrence outcomes. This expands the number of tools that are available to coerce or compel other states to, for example, do their due diligence and respect international standards of behaviour in cyberspace. One example would be conditioning tariffs and market access explicitly (but not exclusively) on cyber behaviour either as a one-off or as part of a broader package – an option that remains largely untested but that the broader turn towards the weaponisation of economic tools for coercion now makes conceivable.

No cyber-conditional tariff has been put in place as a direct retaliation (or threat of retaliation) for a specific cyber incident. However, in 2018, the US came close to implementing such measures. The US Trade Representative (USTR) recommended that US Section 301 tariffs be applied against China due to, among other reasons, China's conduct and support of 'cyber intrusions into U.S. computer networks to gain access to valuable business information'.[38] In the end, USTR imposed four rounds of tariffs on about $370-billion worth of imports from China.[39] In 2024, President Joe Biden's administration applied 25% tariffs on ship-to-shore cranes from China,[40] following reports of Chinese pre-positioning on US critical infrastructure, especially port equipment.[41]

In both cases, tariffs are used to impose costs and constrain the adversary from maintaining market access and profitability. However, these are states that can bear the brunt of these frictions without changing behaviour. Therefore, the use of retaliatory tariffs in response to malicious cyber activity might have limited effects on adversaries. Instead, they may prove to be more effective in managing relationships

38. Office of the United States Trade Representative (USTR), 'Section 301 Fact Sheet', March 2018, <https://ustr.gov/about-us/policy-offices/press-office/fact-sheets/2018/march/section-301-fact-sheet>, accessed 22 June 2026.
39. Karen M. Sutter, 'Section 301 and China: The U.S.-China Phase One Trade Deal', InFocus 12125, Congressional Research Service, 21 May 2026, <https://www.congress.gov/crs-product/IF12125>, accessed 10 June 2026.
40. Ian Saccomanno, Earl Comstock and Gregory Spak, 'USTR Issues Final Section 301 Actions in China Shipbuilding Investigation', White & Case, 12 May 2025, <https://www.whitecase.com/insight-alert/ustr-issues-final-section-301-actions-china-shipbuilding-investigation>, accessed 23 June 2026.
41. New Jersey Cybersecurity and Communications Integration Cell, 'China-Linked Cyber Operations Targeting US Critical Infrastructure', <https://www.cyber.nj.gov/threat-landscape/nation-state-threat-analysis-reports/china-linked-cyber-operations-targeting-us-critical-infrastructure>, accessed 23 June 2026.

© Royal United Services Institute

with other states that might be complacent towards or even supportive of adversaries and/or other kinds of malicious cyber activity.

Both moves, however, run into the same constraint. Economic instruments impose meaningful cost only when applied collectively and consistently. That is why the effort proposed by this multilevel framework is to enable cyber tools to be further refined, non-cyber tools to be used more purposefully to support wider efforts to slow and disrupt malicious cyber activity, and the avenue for cross-thematic tools sequenced so that states use multiple levers to impose costs (or the threat thereof) on adversaries across all areas of statecraft.

## Conditionalities for Cyber Capacity Building

As noted in the framework, cyber capacity building (CCB) is a foundational enabler for all tools, whether defensive and/or proactive/offensive. It encompasses skills, workforce, resources, tooling, and access to information and intelligence. Supporting other countries' development through partnerships or sustained 'raising the bar' efforts can be a direct avenue for achieving deterrence outcomes – provided that support is consistent, needs-based and continuous. Participants for this study noted that support should be offered and structured so that it responds to a framework of conditionalities.

The imposition of conditionalities is not a novel element of international finance and development assistance. CCB could draw on that experience to ensure that cyber is more integrated into multilevel strategies for shaping behaviour in cyberspace. Some examples are worth noting. First, the financial conditionality practised by organisations – such as the International Monetary Fund[42] and the World Bank[43] – already include disbursement in tranches, provided the recipient meets agreed and verifiable steps.[44] Second, there are political or governance conditionalities. One example is the EU's 'more for more' [45] approach, under which 'the EU develops stronger partnerships with those neighbours that make greater progress towards democratic reform'. Deeper cooperation is also reflected in enhanced assistance and market access, among other things. The logic of 'more for more' is an example of inducements for CCB and behaviour/norms alignment.

42. IMF, *Operational Guidance Note on Program Design and Conditionality*, Policy Paper No. 2024/004 (Washington, 2024).
43. World Bank, 'Development Policy Financing (DPF)', 14 July 2026, <https://www.worldbank.org/en/what-we-do/products-and-services/financing-instruments/development-policy-financing>, accessed 23 August 2026.
44. For example, the IMF notes that the elaboration and presentation of clear strategies – tailoring policies to country circumstances and capacity, and linking them clearly to programme goals in the context of the authorities' broader objectives – can enhance programme ownership and implementation. IMF, 'Principles of Conditionality', 9 January 2006, <http://imf.org/external/np/pp/eng/2006/010906.pdf>, accessed 23 August 2026.
45. European Parliament, 'The European Neighbourhood Policy', <https://www.europarl.europa.eu/factsheets/en/sheet/170/the-european-neighbourhood-policy>, accessed 22 July 2026.

© Royal United Services Institute

**Figure 4:** Conditionalities and Inducements for CCB

De-escalation: the gradient is reversible – verified improvement moves the relationship back up at every tier

| | Harmonious | Drift | Material Concern | Serious Breach | Rupture |
|---|---|---|---|---|---|
| **Observed Behaviour** (the input) | Meets commitments; aligns on norms; cooperates in good faith on shared threats and other cyber-related activities/initiatives | Tolerance of low-level activity; missed benchmarks; slow implementation; ambiguous signals (slippage, not bad faith) | Clear failure to meet commitments; governance backsliding; tolerating activity from territory | Active harbouring or obstruction; complicity; commitments abandoned | Sustained complicity or hostile alignment; relationship no longer tenable |
| **Calibrated Measure** (the response) CARROT → STICK | **Expanded Provision** Standard delivery (expected) and enhanced training, tooling, and/or intelligence access as sustained support and relationship develops; operational partnership including, for example, hunt-forward deployment, as a positive inducement | **Enhanced Monitoring** Communication with recipient; reporting requirements (if necessary); technical assistance to recover (positive inducement, not penalty) | **Explicit Conditionality** Future tranches/ instalments tied to verifiable steps; pause on new commitments; formal démarche | **Suspension** Pause specific programmes; withdraw sensitive components (tooling, intelligence); public signalling | **Termination** Full withdrawal; redirect resources to neighbours; coordinate with allies to prevent capacity shopping |
| **Relationship Status** (the consequence) | FULL PARTNER | UNDER REVIEW | CONDITIONAL | SUSPENDED | SEVERED |

Source: The authors.

Discussions about conditionalities should be calibrated to the type of funding being offered:

- **Official Development Assistance (ODA)**
  Needs to meet at least three criteria.[46] First, it must come from official government sources. Second, its primary objective should be the economic development and welfare of developing countries. Third, it must be concessional (a grant, or a loan with a grant component). ODA funding for explicit cyber deterrence might be challenging as it may be seen as securitising aid/assistance – although they need not be labelled as such. This would be against the OECD peace and security eligibility rules that exclude ODA for military, security and weapons development purposes. Conditionalities would need to be calibrated to 'raising the bar' components of the framework.

46. OECD, 'Official Development Assistance – Definition and Coverage', <https://www.oecd.org/en/topics/sub-issues/oda-eligibility-and-conditions/official-development-assistance--definition-and-coverage.html>, accessed 23 July 2026.

© Royal United Services Institute

- **Other official flows**
  Official government spending that does not meet ODA rules either because its purpose is not (strictly) development or because it is not sufficiently concessional. This may include export credits, official investment on commercial terms and – potentially – some security-related spending. Conditionalities could be more openly tied to the provider's interests and shared vision of responsible cyber behaviour.
- **Security and defence assistance**
  Primarily focused on security and defensive capacity of partners. This funding could include training, cooperation with defence, and equipment. Given the scope, conditionalities could be even more explicitly tied to shared views of norms, the partner's conduct in cyberspace, alignment and reciprocity.
- **Non-concessional / commercial, blended finance, guarantees**
  Not focused on states or concessions. This funding is investment rather than primarily development oriented, and may include loans, public–private blends and risk guarantees. Conditionality is contractual and may incorporate expectations on standards, interoperability, trusted vendors and supply chain requirements.

A multilevel deterrence approach to CCB looks at the framework, explores the different modalities of funding at a state's disposal (as above) and designs a strategy for how to properly calibrate conditionalities across funding types in the event of escalation, changes in behaviour or non-compliance. The same applies to working back the escalation with positive inducements to build trust and make sure conditionalities are coupled with incentives for closer cooperation.

More robust or explicit CCB conditionalities frameworks run the risk of producing a chilling effect,[47] leading potential partners to decline to cooperate if conditionalities are burdensome and negatively framed (rather than framed as positive inducements). The received wisdom in the field of development is that heavy, externally imposed conditions tend to produce worse and less durable outcomes than reforms that a partner owns, and that overloading support with conditions can defeat its purpose.

Another risk is that it leads potential grantees to engage in capacity shopping. A partner faced with onerous conditions from one provider may seek cyber capacity elsewhere, including from states that do not attach governance and/or behavioural expectations. This is why the withdrawal of support only imposes cost if it is coordinated with like-minded providers and is carefully and cautiously calibrated. Unilateral conditionality against a backdrop of willing alternative suppliers imposes little cost – at least in the medium term – on third countries.

47. Patryk Pawlak and Panagiota-Nayia Barmpaliou, 'Politics of Cybersecurity Capacity Building: Conundrum and Opportunity', *Journal of Cyber Policy* (Vol. 2, No. 1, 2017), pp. 123–44.

© Royal United Services Institute

A related risk is that conditionality can invite a countervailing system of incentives. Rival states may deliberately position themselves as unconditional alternatives, offering support precisely to undercut the influence that Western conditionality is intended to create.

All these potential risks are – and should continue to be – calibrated depending on the relationship, strategic goals and willingness to cooperate, among other factors.

## The Risk of Institutional Blindness

The previous section shows how states might plan the distribution and sequencing of non-cyber tools for deterrence outcomes. However, two assessments of behaviour might point in opposite directions for the same country. Consider a state with genuine capacity deficits which is also, due to inaction, harbouring criminal infrastructure operating against the assessing state's networks. On the CCB gradient, this state might be in Tier 2 and might benefit from inducements to enable it to react. On the economic gradient, the state might be placed in Tier 3 and warrant financial friction or designations depending on complacency and history of cooperation (or lack thereof).

Each reading measures discrete aspects, so both can be correct at the same time. What must not happen is a situation where a donor country's ministry of development increases assistance while its ministry of finance/commerce applies scrutiny and its foreign ministry issues a démarche for inaction, while none is aware of the actions taken by the others. The recipient would observe the incoherence and draw the reasonable conclusion that no single signal is authoritative. Therefore, this may weaken the overall signal and action required to induce behavioural change (in this case, cooperative).

Deciding which instrument leads, which is held in reserve and what the assistance is explicitly conditioned on is not simply a bureaucratic refinement. Isolated activities that lack mandated whole-of-government oversight, a coordinating function or incentives for cross-ministerial/departmental work are not incrementally more potent – they are ineffective.

The coordination of the sequencing and layering of tools is crucial in a whole-of-government approach to deterrence.

© Royal United Services Institute

## Layering Costs and Tools Over Time

The previous section assessed how intensity of tool use and sequencing should be matched to behaviour and context. This section looks more closely at how tools might compound against a particular adversary over time.

This section emphasises some critical factors that should be considered to establish and pursue effective campaigning. Ultimately, the aim is to achieve cyber deterrence outcomes.

### Drawing and Communicating Red Lines

A layered approach where multilevel actions seek to achieve deterrence outcomes would combine proactive and sustained measures (calibrating raising the bar and imposing costs below Tier 3) with a clear and complementary demarcation of red lines – unacceptable behaviour – that would trigger scalable or proportionately stronger measures. The credibility of any threat to retaliate depends on clearly communicating and outlining – ideally publicly – the sorts of cyber breaches that are completely unacceptable for the host state, even if they are 'on' or 'below' the threshold of conflict.

A departure from strategic ambiguity may appear counterintuitive or uncomfortable. However, drawing red lines serves notice to adversaries and provides a foundation for the use of tools in the event that those red lines are crossed. As one workshop participant underlined, 'not everything is deterrable. It isn't clear if we're trying to deter specific attacks or the volume … not everything can be a red line. If everything is, nothing is'.[48]

There have been few examples of red lines being drawn overtly in the context of cyber intrusions. The clearest is Biden's publicly reported remarks at a July 2021 summit with President Vladimir Putin, in the aftermath of the Colonial Pipeline incident. Referring to '16 sectors' designated as critical by the US Homeland Security Department, Biden emphasised that destructive cyber operations (as opposed to espionage) would be unacceptable to the US and that the US could 'respond with cyber'.[49] Both presidents expressed a desire to task consultations on cyber security between the two countries, although it is unclear that these were ever institutionalised. In a speech the following month, Biden noted that 'if we end up in a war, a real shooting war with a major power, it's going to be as a consequence of a cyber breach of great consequence'.[50]

48. Information provided by workshop participant, 27 May 2026.
49. Vladimir Soldatkin and Humeyra Pamuk, 'Biden Tells Putin Certain Cyber Attacks Should Be "Off-Limits"', *Reuters*, 16 June 2021.
50. Katrina Manson, 'Biden Warns Cyber Attacks Could Lead to a "Real Shooting War"', *Financial Times*, 28 July 2021.

© Royal United Services Institute

These are the clearest examples – in the public domain – of cyber red lines and threats of retaliatory action up to, and including, an armed conventional response. Biden emphasised them in a March 2022 statement on cyber security[51] – after the commencement of the Ukraine conflict – noting that 'my administration is reiterating those warnings based on evolving intelligence that the Russian government is exploring options for potential cyberattacks'.

However, they have not been emphasised by US administrations or agencies since that statement. Nor were they corroborated or shared by Allies and partner countries, which suggests that declaratory tools used only by one state can fall short of their potential for triggering multilevel action. A practitioner interviewed acknowledged that the UK had not signalled red lines, and noted that it would be ideal if 'thick' red lines were drawn as part of a coherent position.[52] At an international institutional level, the closest example of collective signalling might be the repeated suggestions that NATO's Article 5 might be triggered[53] by a significant cyberattack, or through a country's position on how international law applies to cyberspace. This position arguably maintains strategic ambiguity, and it is likely that a high threshold (that is, an act of war) would be required to trigger a forceful collective response. Therefore, the cyber red line drawn by NATO arguably befits a framing of deterring general armed conflict, rather than a cyber deterrence policy that includes incidents that are on or below the threshold.

Communicating thresholds (and intent) is essential. The tools outlined in this paper serve both to deliver or facilitate achieving deterrence outcomes, and to communicate to an adversary. As scholars Erica Lonergan and Mark Montgomery note in a 2021 article,[54] signalling is an 'essential' element of prospective cyber deterrence: 'the deterring state must communicate to the target its expectations about behaviour and consequences for defection in a way that is appropriately understood by the target'. Ultimately, established red lines would give clarity and purpose to the communication that is intended through the use of individual and layered deterrence tools.

51. White House, 'Statement by President Biden on Our Nation's Cybersecurity', 21 March 2022, <https://bidenwhitehouse.archives.gov/briefing-room/statements-releases/2022/03/21/statement-by-president-biden-on-our-nations-cybersecurity/>, accessed 23 July 2026.
52. Author interview, 3 December 2025.
53. NATO, 'Collective Defence and Article 5', 12 November 2025, <https://www.nato.int/en/what-we-do/introduction-to-nato/collective-defence-and-article-5>, accessed 2 July 2026.
54. Erica Lonergan and Mark Montgomery, 'What is the Future of Cyber Deterrence?', *SAIS Review of International Affairs* (Vol. 41, No. 2, Fall–Winter 2021), pp. 61–73.

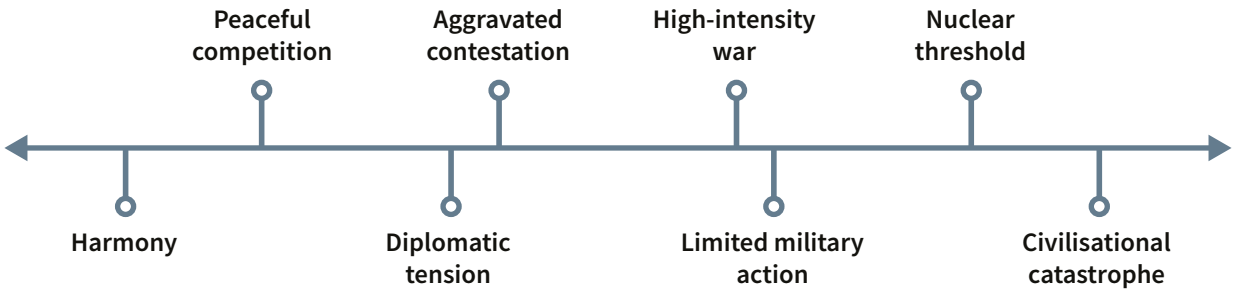
© Royal United Services Institute

## Control the 'Escalation Ladder' Rather Than Stop All Cyber Incidents

As previously noted, it is not possible to prevent all cyber incidents. If the cyber deterrence bar is set at the level of stopping every incursion, it arguably becomes redundant and most likely impossible. Instead, as per the previous subsection, stakeholders should identify the threats that they believe must be stopped and formalise this by drawing and communicating the red lines.

Cyber deterrence tools deployed on the basis of these red lines – and used in combination with a backdrop of persistent cyber engagement – can influence or moderate adversarial cyber behaviour. This includes behaviour below the threshold of armed conflict. Figure 5 illustrates a generic escalation ladder. Arguably, 'cyber deterrence' as a standalone deterrence framing is most applicable at levels below limited military action. Once military action commences, a general conventional (and nuclear, where applicable) deterrence framing would logically supersede and subsume a cyber one.

**Figure 5:** General Escalation Ladder




Source: The authors.

During periods of peaceful competition, diplomatic tenson and aggravated contestation, adversaries may conduct or condone a range of cyber incursions into the deterring country's networks. This may include pre-positioning, data exfiltration and disruptive attacks that are below (or, in egregious cases, near) the threshold. Many cyber incidents will not have a direct impact on the general escalation ladder between the offending and deterring states; although some will if the impacted state decides to treat it as an escalatory incident.

© Royal United Services Institute

### Layering Costs is not a 'One Size Fits All' Question

To support effective layering of costs, cyber deterrence campaigns need to be bespoke for specific state actors. A tool (such as public attribution) that is effective against one adversary may not be effective at altering the behaviour of another. As one workshop participant highlighted, 'cost is in the head of the adversary'. This means that the deterring state should identify what 'pain for them' is and design a campaign on this basis.[55]

Seemingly ineffective tools may still have a place, even if an adversary does not see itself incurring a cost when they are used against it. For example, a public attribution against a GRU unit is unlikely to result in meaningful behavioural change within that unit or indeed any other part of the Russian offensive cyber ecosystem. However, the attribution might serve as a legitimising or facilitative tool for other – more effective – tools. For instance, a public attribution may bolster a legitimising narrative that encourages a broader coalition of states to engage in economic, diplomatic or other measures against Russia that enact costs on a collective basis.

Layering costs in a tailored manner also enables granular assessments of effectiveness. This could be observed through a range of data points. A key data point – indeed, one that links with the purpose of deterrence – would be observed changes in behaviour over time. Another indicator could be public or private discussion of the tool's use and/or effects among stakeholder groups in the adversary country. Observed changed behaviour – or the lack thereof – can inform decision-making in the deterring country, to determine whether a campaign needs to be modified.

## Conclusion and Recommendations

This project and its engagement with practitioners have revealed a groundswell of clear earnestness to do more with existing tools, to try new methods and to combine them more effectively for the purpose of reducing the incidence of cyber breaches against core services and institutions. There is significant scope for practitioners to apply a framework of multidomain campaigning that could – over time – create the conditions in which cyber deterrence may be achieved as an outcome. This outcome could be achieved by using a combination of raising the bar, imposing costs, offering inducements and leveraging the use of enablers; it can make use of tools that are not predominantly and inherently 'cyber'.

This paper and other research frames cyber deterrence as an outcome rather than a strategy. This approach may help NATO and EU member states to escape the common misconception: first, that cyber can be effective as a deterrence toolkit in isolation; and

55. Information provided by workshop participant, 27 May 2026.

© Royal United Services Institute

second, that cyber deterrence should carry over the 'baggage' of traditional deterrence strategies that simply will not neatly align with the fifth sphere of power projection.

The following recommendations are designed for NATO and EU member states and partners. This article acknowledges that other governments might find them, as well as the framework, a welcome challenge or provocation to their domestic/international discussions. The focus is on cyber deterrence outcomes and at least five desired outcomes. These can enable and operationalise the disruption, detection and reduction of malicious state-linked cyber activity. In accordance with the framework, these outcomes also reflect recommendations of actions that can be taken to enable, raise the bar, enhance inducements and/or impose costs/proactive posture.

## Desired Outcome 1: A State is Aware of the Tools at its Disposal and Uses Them Coherently (Domestically, Regionally and/or Internationally)

**Function(s):** Enablers

**Relates to deterrence outcomes:** restored Allied freedom of action

1. Designate a coordinating function with a whole-of-government mandate to hold the national tool map, identify cross-ministerial incoherence and arbitrate which instrument leads. Arrangements could vary, as this coordinating function could be permanent or temporary; it could be designated to a specific body, an assessment to be conducted by a department, or a function to be performed by a cross-governmental group.
2. Maintain a national register of instruments mapped to the four functions, recording owner, legal basis, lead time and known dependencies and conflicts between tools.
3. Conduct national assessment of the levels of maturity and propensity of use of cyber and non-cyber tools for cyber deterrence outcomes.

© Royal United Services Institute

## Desired Outcome 2: A State Provides Clearer Indications of Thresholds and Resulting Actions

**Function(s):** Enablers Imposing Costs

**Relates to deterrence outcomes:** threshold compliance; escalation ladder control

1. Publish a short threshold statement naming a small number of categories of cyber activity that the state will treat as unacceptable, and state explicitly that the response may be drawn from any instrument of statecraft, not only cyber.
2. Coordinate threshold statements with a coalition before publication and secure prior commitments to corroborate them.
3. Whenever possible, pre-agree – and possibly at higher classification levels – the menu and sequencing of instruments that a breach of each declared threshold triggers, and the decision authority for each.
4. Identify ways of publicly communicating the implementation of proactive measures across the toolkit, especially in more sensitive areas such as offensive cyber operations.

## Desired Outcome 3: A State or a Group of States is Able to More Rapidly Mobilise for Multilevel Collective Action in Areas of Shared Interest or Tool-Use Maturity

**Function(s):** Enablers Imposing Costs Benefits/Inducements

**Relates to deterrence outcomes:** freedom of action; third-party behavioural change; (potential) higher adversary cost per operation

1. Establish new coalition-building mechanisms or use existing collective response channels and mechanisms for designations and attribution statements while calibrating partnerships based on variables such as shared threat, type of attack, targeted entity/sector, and/or regional or cross-regional concern.
2. Assess critical constraints for each tool considering at least the following elements: legal basis; evidentiary standard; concentrated exposure; enforcement capacity; and reversibility (key for ensuring inducements can be provided, depending on the tool). Plan adjustments to enhance freedom of action based on assessment.
3. Explore possibilities of mainstreaming country-specific sanctions regimes for hybrid threats to a broader tool that could be directed against multiple states engaging in such activities.
4. Expand the economic toolkit in at least two directions: first, scale, from named entities to serial and sectoral packages; and second, scope, with cyber conduct conditions written into market access, tariffs implementation, procurement, export licensing and trade preference/conditionalities at design and implementation stage.

© Royal United Services Institute

## Desired Outcome 4: Partnerships with Third-Party Countries Leads to Behavioural Change

**Function(s):** Raising the Bar | Benefits/Inducements | Enablers

**Relates to deterrence outcomes:** third-party behavioural change; denial of strategic advantage; higher adversary cost per operation; enhanced freedom of action

1. Calibrate economic instruments based on relationships and where they can effectively change behaviour: against adversaries that are able to absorb them, use them for coalition-building and legitimising effect; and against middle-ground states, reserve the expectation of behavioural change for complacent and harbouring states.
2. Build the enabling structures for proactive partnerships (for example, HFOs) including host-nation consent frameworks, standing teams, intelligence and operational arrangements and a prioritised country list.
3. Calibrate capacity-building conditionality by funding type, pair every condition with a positive inducement and coordinate any withdrawal of support with like-minded providers to prevent capacity shopping.

## Desired Outcome 5: States Can Individually and/or Collectively Sustain Pressure on Adversaries

**Function(s):** Raising the Bar | Imposing Costs

**Related to deterrence outcomes:** higher adversary cost per operation; denial of strategic advantage; escalation control

1. Develop/refine tailored approached to adversaries based on the assessment of context and tools to apply sustained and cumulative pressure to reduce their strategic advantage in cyberspace.
2. States identify areas of cooperation and complementarity based on national assessments of propensity and desirability for using of specific tools (see the third bullet in Desired Outcome 1) to maximise strengths and sustain pressure in a collective manner through multitool use.
3. Review campaigns against outcome indicators.
4. Plan campaign strategy for multiple scenarios considering potential changes in context (competition, crisis, conflict) and cooperative ties/mechanisms needed (diplomatic, technical, operational) that can be leveraged given potential change (see Desired Outcome 1).

© Royal United Services Institute

# Acknowledgements

The authors would like to thank their peer reviewers for the exceptional feedback, along with RUSI's internal Research Editorial and Publications teams, Microsoft for supporting this research, all interviewees and workshop participants for their sustained collaboration and openness, and NATO, EU organisations and other member states for the opportunity to brief and exchange views on this matter.

# About the Authors

**Louise Marie Hurel** is a Senior Research Fellow at RUSI's Cyber and Tech team, where her work focuses on cyber deterrence, responsible cyber behaviour, cyber diplomacy, AI cybersecurity and assurance, and Big Tech politics. Prior to joining RUSI, she led Igarapé Institute's Digital Security Program, coordinating efforts to connect national, regional and international cyber policy discussions and worked as a consultant for the United Nations on cyber and data security. She is a Senior Research Associate at Virtual Routes and an advisory board member of the Global Forum of Cyber Expertise, Carnegie Endowment's Partnership for Countering Influence Operations and the Centre for Information Resilience. In 2024, Louise was appointed as civil society expert in Brazil's inaugural National Cyber Committee and, in 2022, she founded the Latin American Cybersecurity Research Network. She has a PhD on Data, Networks and Society and an MSc in Media and Communications from the London School of Economics and Political Science.

**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. Prior to joining RUSI, he was a Lecturer in Security and Intelligence at the University of Kent. In this role, his research focused on the convergence of networked technologies and (inter)national governance. He convened a popular research-led module entitled 'Governance and War in Cyberspace', and supported the development of the university's Institute of Cyber Security for Society as an Organisational Lead. Previously, he was a Lecturer in International Relations at Nottingham Trent University. Gareth holds a PhD in International Relations (Security Studies), completing an original thesis on the spectre of cyberterrorism in 2018. He also holds an MA in International Security and a BA in International Relations and Modern History.

© Royal United Services Institute

## 195 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 195 years.

© The Royal United Services Institute for Defence and Security Studies

RUSI is registered as a charity in England and Wales

Charity number: 210639

VAT number: GB752275038