Research Paper

International Security Programme

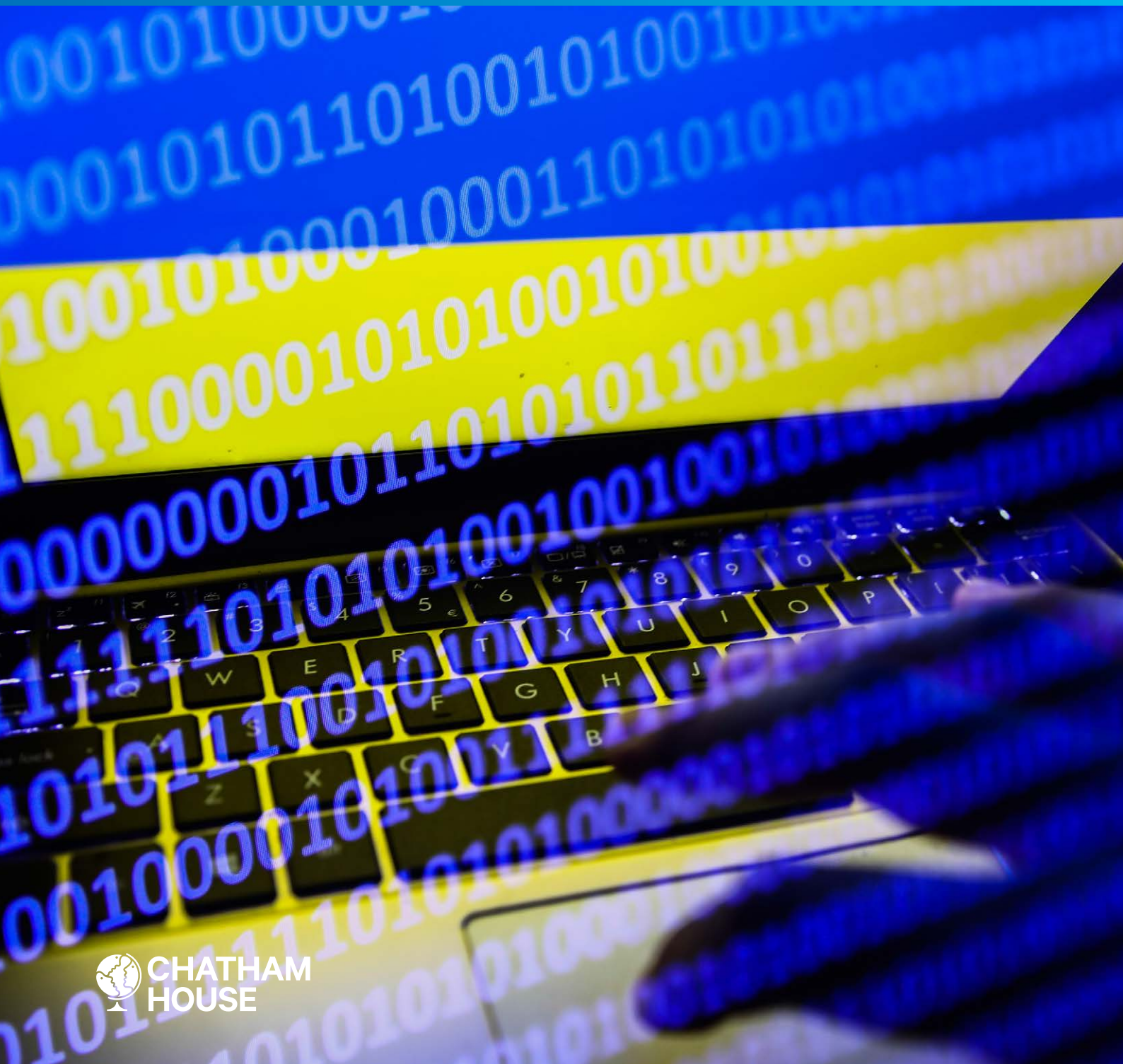
International Law Programme

March 2026

Holding state-sponsored hackers and other cyber proxies to account

Lessons from tackling proxies in Russia's war on Ukraine

Joyce Hakmeh, Harriet Moynihan and Nayana Prakash



CHATHAM HOUSE

Chatham House, the Royal Institute of International Affairs, is a world-leading policy institute based in London. Our mission is to help governments and societies to build a secure, sustainable, prosperous and just world.

Contents

Summary

- **Russia's invasion of Ukraine demonstrates that cyber operations and online influence campaigns are now integral to modern warfare**. Deployed alongside conventional military force, these tactics entail the extensive use of proxies – criminal groups, companies, hacktivists and semi-autonomous actors operating with varying degrees of state direction, tolerance or alignment.
- **The wide variety of Russian or Russia-linked cyber proxies**, differing in their organization, motivation and relationship to the state, **creates a spectrum of threat actors that complicates attribution** and benefits Russia by enabling calibrated deniability and facilitating the evasion of sanctions.
- **Despite its scale and persistence, Russia's cyber campaign against Ukraine has not achieved the strategic effects Moscow anticipated.** Ukraine's government continues to function, its military communicates, and its critical infrastructure – while repeatedly targeted and damaged – has not been decisively disabled. The relative failure of Russian tactics reflects the substantial improvement in Ukraine's cyber defences since 2014, extensive Western technical and intelligence support for Ukraine, and the adaptive resilience of Ukrainian institutions.
- **Various rules of international law are relevant to proxy activity; these include international humanitarian law (IHL) and rules on state responsibility and due diligence.** States have agreed, as part of the UN Framework for Responsible State Behaviour in Cyberspace, that international law applies in the cyber context, and that some of the UN cyber norms are relevant to the activities of proxies. Proxy actors who commit cyber-enabled international crimes may also face individual criminal liability.
- **High thresholds for attributing non-state actor conduct to states mean that Russia often evades responsibility** for proxy operations under traditional state responsibility frameworks. Yet even when attribution to Russia is not possible, states can prosecute identifiable individuals (as well as imposing reputational costs and travel restrictions). States increasingly take law enforcement action as part of broader strategies to disrupt cyber activity by proxy actors, alongside political, diplomatic and economic measures. International law frameworks dealing with mercenaries, foreign fighters and transnational organized crime also offer useful lessons for policymakers seeking to hold Russia responsible for harbouring cyber proxies.

- **Current responses by Ukraine and its allies to proxy activities have delivered tactical successes, but have not strategically degraded the capabilities of hostile cyber actors.** Response mechanisms and options remain fragmented across legal, economic and operational domains. Proxies exploit this fragmentation by evading accountability through jurisdictional loopholes and functional gaps. Even after disruption or apparent deactivation/dissolution, proxies are often able to reconstitute themselves quickly and resume activity. This reflects the fact that state and multilateral responses frequently fail to target the enabling ecosystems – including hosting infrastructure, payment processors, cryptocurrency exchanges and technology suppliers – on which proxy operations depend.
- **Achieving strategic coherence in the fight against cyber proxies – whether those linked to Russia or to another state – requires more coordinated action** across legal, economic and operational domains. Depending on the context and potential victim(s), coordination at minimum might usefully include the US, the UK, the EU, Australia, Canada and Japan. It would entail pairing criminal prosecution with synchronized multilateral sanctions targeting infrastructure providers; deploying operational disruption campaigns that generate compounding effects; and leveraging existing initiatives (such as the Pall Mall Process) to restrict the tools available to cyber proxies.
- **A hierarchy of action** – core strategic levers that degrade capacity, amplifiers that multiply pressure, and enablers that sustain long-term effectiveness in tackling cyber proxies – **would offer a pragmatic path forward that reflects political realities without awaiting universal institutional reform**.
- **Holding cyber proxies to account also requires the active engagement of the private sector.** Technology companies, hosting providers and financial services firms control much of the infrastructure that proxies exploit to conduct operations, while critical national infrastructure operators are among the primary targets of hostile cyber activity. The development of formalized engagement frameworks, with clear obligations and liability protections, would help private companies become more active contributors to collective defence against cyber proxies.

01 Introduction

Russia's full-scale invasion of Ukraine in 2022 marked a new era of hybrid warfare, with cyber operations and proxy actors playing a persistent strategic role. This paper examines how – and how effectively – the international community can hold those actors accountable.

On 24 February 2022, hours before Russian tanks crossed into Ukraine, a cyberattack disabled tens of thousands of satellite modems across Ukraine and parts of Europe.[1] The Viasat incident disrupted Ukrainian military command-and-control systems at a critical moment, signalling that Russia's invasion would unfold not just on the ground but in cyberspace. Over the following weeks and months, many of the subsequent cyber operations, often linked to a mixture of Russian state agencies and cyber proxies, deployed wiper malware against Ukrainian government networks, launched distributed denial-of-service (DDoS) attacks against critical infrastructure, and flooded social media with disinformation. For many observers, these events appeared to validate predictions that cyber would become a decisive dimension of the conflict, potentially crippling Ukraine's ability to defend itself and generating spillover impacts on Western states supporting its defence.[2]

A critical but often under-analysed dimension of Russia's cyber campaign has been its extensive use of proxies. This paper uses the term 'cyber proxy' to encompass a wide variety of actors – from units formally tasked by state intelligence services, through criminal groups operating with state tolerance, to commercial enterprises – whose relationships with the Russian state vary considerably in nature and degree, with significant implications for how accountability mechanisms are designed and applied.

1 Viasat (2022), 'KA-SAT Network cyber attack overview', 30 March 2022, https://news.viasat.com/blog/corporate/ka-sat-network-cyber-attack-overview.
2 Cerulus, L. and Scott, M. (2022), 'Cyber tensions rise as West fears invasion of Ukraine', POLITICO, 14 February 2022, https://www.politico.eu/article/cyber-tensions-rise-as-west-fears-ukraine-invasion.

At one end of the spectrum sit non-state actors commissioned by 'advanced persistent threats' (APTs) such as Russia's intelligence services (see Table 1); APT-commissioned proxies retain partial operational autonomy but execute tasks aligned with state objectives. At the other end are commercial enablers: private companies and contractors that willingly provide infrastructure and services to malicious actors, motivated by profit or ideological alignment. These include so-called 'bulletproof hosting' providers, virtual private network (VPN) services offering anonymity, IT contractors developing custom tools, and cryptocurrency services facilitating money laundering.

Between these poles sits a diverse middle ground: ransomware collectives such as Conti, hacktivist groups like Killnet (both active in the conflict's early phase before fragmenting into affiliated networks and successor brands), criminal networks, contractors and semi-autonomous groups. Many of these actors, while not openly directed by the Russian state, have operated with varying degrees of tacit approval or ideological alignment; some have acted entirely independently, motivated by financial gain or political sympathy. Given this diversity, the relationships between cyber proxies and the Russian state often resist easy categorization.

Across this spectrum of relationships and actor types, the use of proxies expands Russia's cyber reach, provides plausible deniability for perpetrators and the political leadership, makes attribution of cyberattacks and other hostile operations difficult, and helps insulate both the Russian state and individual actors from sanctions – even where, as with APT-commissioned proxies, the state remains the principal actor behind the operation.

Why Russian cyber operations have not achieved strategic effects

Four years into the war, Ukraine still functions. Its government operates, its military communicates and its infrastructure – while repeatedly targeted and damaged – continues to provide essential services, often under emergency conditions. Russian cyber operations have been relentless and damaging, imposing real costs on Ukrainian society and military operations. But Russian cyber activity has not achieved the strategic effects Moscow appears to have anticipated.[3]

Several factors explain this. First, Ukraine has substantially improved its cyber defences since 2014, building on lessons from repeated Russian attacks. Investments in resilient networks, distributed infrastructure, cloud-based services and institutionalized incident response have significantly reduced the impact of many Russian operations, forming a strong domestic foundation for cyber resilience.

3 Fendorf, K. and Miller, J. (2022), 'Tracking Cyber Operations and Actors in the Russia-Ukraine War', Council on Foreign Relations, 24 March 2022, https://www.cfr.org/articles/tracking-cyber-operations-and-actors-russia-ukraine-war.

Second, Western support during the war has significantly enhanced Ukraine's ability to detect, mitigate and recover from cyberattacks, often far more quickly than Russia has anticipated.[4] Such support includes: cyber assistance from the US, Canada, the UK, Estonia and others; coordinated civilian cyber capacity-building through the Tallinn Mechanism;[5] extensive public–private defensive operations; and private sector threat intelligence and initiatives, such as the Cyber Defense Assistance Collaborative (CDAC).[6] Finally, Russia's own operational assumptions have shifted as the war has endured far beyond Moscow's initial expectations of a swift victory.

As the conflict has evolved into a protracted war of attrition, Russian cyber activity has changed tack. It has increasingly sought to deliver direct battlefield advantages. Intelligence collection, signals monitoring and real-time targeting support have become priorities. Operations have included compromises of mobile devices used by Ukrainian military personnel, exploitation of encrypted communications platforms, and deployment of malware designed to support operational intelligence and tactical coordination.[7] At the same time, Russia has retained – and occasionally employed – the capability to conduct large-scale attacks against critical national infrastructure, whether through sustained missile and drone strikes on Ukraine's electricity network[8] or through cyberattacks such as the 2023 incident that temporarily disabled Kyivstar, Ukraine's largest telecommunications provider.[9]

Russian cyber operations in Ukraine have been neither the war-defining force some anticipated, nor the strategic irrelevance others dismissed.

Parallel to these technical operations, Moscow has pursued extensive cyber-enabled influence campaigns, deploying coordinated networks of inauthentic accounts, botnets and fabricated content across social and other digital platforms to spread pro-Russian narratives, undermine Ukrainian morale and weaken Western political support for Kyiv's defence. These information operations are tailored to distract, divide and destabilize both Ukrainian and wider international audiences, and have been particularly effective at exploiting rapidly shifting perspectives among traditionally allied Western nations. Russian operations have flooded European websites and social media with untrusted content and have made it difficult for citizens to identify authentic sources of information. This dual approach – blending

---

4 Montgomery, M. and Fixler, A. (2023), 'Building Partner Capabilities for Cyber Operations', Foundation for Defense of Democracies, 27 July 2023, https://www.fdd.org/analysis/2023/07/27/building-partner-capabilities-for-cyber-operations; and Smith, B. (2022), 'Digital technology and the war in Ukraine', Microsoft On the Issues blog, 28 February 2022, https://blogs.microsoft.com/on-the-issues/2022/02/28/ukraine-russia-digital-war-cyberattacks.
5 Global Affairs Canada (2023), 'Tallinn Mechanism', 19 December 2023, https://www.international.gc.ca/world-monde/issues_development-enjeux_developpement/peace_security-paix_securite/tallinn-mechanism-mecanisme-tallinn.aspx?lang=eng.
6 https://crdfglobal-cdac.org.
7 Black, D. (2024), 'Russia's Cyber Campaign Shifts to Ukraine's Frontlines', RUSI Commentary, 22 July 2024, https://www.rusi.org/explore-our-research/publications/commentary/russias-cyber-campaign-shifts-ukraines-frontlines.
8 Rainsford, S. (2026), 'Record number of missiles hit Ukraine leaving thousands with no heating in -20C', BBC News, 3 February 2026, https://www.bbc.co.uk/news/articles/cpwng25114ro.
9 Parker, J. (2023), 'Ukraine mobile network Kyivstar hit by "cyber-attack"', BBC News, 12 December 2023, https://www.bbc.co.uk/news/world-europe-67691222.

technical cyber operations with influence activities – showcases how Moscow continues to view cyber as a strategic lever that can be applied selectively for tactical, coercive and cognitive effects.

Taken together, these dynamics illustrate a complex reality: Russian cyber operations in Ukraine have been neither the war-defining force some anticipated, nor the strategic irrelevance others dismissed. Rather, they reflect a persistent, adaptive – if sometimes uncoordinated – effort to integrate cyber capabilities with conventional warfare, underpinned both by state units and by proxies.

This paper builds on this analysis to examine Russia's broader cyber approach in Ukraine from 2022 to 2024, with a particular focus on the structure, behaviour and strategic function of what can be termed Russia's cyber proxy 'ecosystem'. A central concern is the question of accountability: how can states meaningfully respond to offensive and malicious cyber operations conducted through proxies that operate in the grey space between state direction, tolerated activity and opportunistic alignment?

Existing responses from Ukraine and its allies to Russian cyber proxies have achieved measurable tactical gains within the particular domains involved. Criminal indictments have named alleged perpetrators and have documented activities, coordinated sanctions have imposed costs on individuals and entities, technical attribution has publicly exposed operations, and disruptions such as the takedown of the LockBit ransomware group (via Operation Cronos) have temporarily degraded prominent threat actors.

However, these measures have not translated into strategic-level success in degrading the proxy ecosystem as a whole. Recent coordinated counter-proxy operations – including Cronos, Endgame and NoName – have achieved measurable tactical impact, with some evidence suggesting significant reductions in ransomware activity following enforcement actions targeting the infrastructure and financial networks on which proxies depend. Yet these gains remain vulnerable to the remarkable ability of many cyber proxies to reconstitute themselves and adapt even after initially successful action against them: indictments and sanctions have only partially constrained threat actors' operations over time, as such actors have often migrated to successor groups or pivoted to alternative methods (such as identity theft and data extortion). Even when specific organizations have been dismantled, the underlying enabling ecosystem of infrastructure providers, cryptocurrency exchanges, technical supply chains and so on has largely persisted. The challenge is not that individual operations fail, but that tactical successes have not yet compounded into systemic degradation of proxies' capabilities.

This fragmentation reflects institutional realities: different Ukrainian and Western intelligence and anti-cybercrime agencies operate under different mandates and legal frameworks both within and across jurisdictions, and Ukraine's international partners have divergent capabilities and approaches. Such separation creates exploitable gaps that adversaries systematically leverage.

The central argument of this paper is that tactical successes cannot substitute for strategic coherence in holding cyber proxies accountable. While different tools and domains require specialized approaches, each response mechanism

must contribute to a unified strategic purpose rather than function in isolation. Achieving accountability demands alignment across attribution, legal, diplomatic and economic tools through sustained international coordination. By analysing how Russia employs proxies across different dimensions – and how Ukraine, its partners and the wider international community have responded – this paper aims to inform the development of more coherent strategies for countering state-aligned cyber proxies not only in the current Russia–Ukraine war but also in future conflicts, where proxies are expected to remain prominent and play a destabilizing role.

Methodology

This paper is carefully confined in scope in order to allow in-depth focus on a particular context involving Russian proxies.

Firstly, our analysis centres on the 2022–24 period in the war on Ukraine. This time frame corresponds with the large-scale escalation of Russian hostilities against Ukraine and the intensification of associated cyber proxy operations. Although cyber activity linked to the conflict extends at least back to 2014, when Russia annexed Crimea and occupied parts of eastern Ukraine, we treat this earlier phase of conflict as contextual background that sheds light on the emergence and evolution of proxy relationships, tactics and capabilities.

The selected time frame therefore represents a concentrated phase of activity in which Russian cyber operations became more visible, diversified and operationally integrated with conventional military campaigns. Focusing on 2022–24 enables an analytical approach that covers a period of high operational tempo, abundant open-source visibility, and extensive public attribution by both governmental and private sector actors. Earlier incidents such as the NotPetya attacks (2017)[10] and the 2015–16 intrusions against Ukraine's power grid[11] demonstrate the long-standing role of Russian cyber operations in Ukraine, but the escalation beginning in February 2022 marked a qualitative and quantitative shift in the frequency, coordination and strategic purpose of such activity.

Although the conflict and associated cyber operations have of course continued beyond 2024, attaching an end date to the period of activity principally covered in this paper also provides a pragmatic boundary for our analysis, ensuring depth over breadth while leaving scope for subsequent longitudinal comparison. Notwithstanding this point, the paper also draws, where relevant, on developments from 2025 and early 2026 – including significant prosecutions, sanctions designations and institutional developments.

Secondly, this paper focuses primarily on cyber proxies operating *in support of* Russia, reflecting the position of Russia as the aggressor state in the ongoing

10 Greenberg, A. (2018), 'The Untold Story of NotPetya, the Most Devastating Cyberattack in History', *Wired*, 22 August 2018, https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world.
11 Cybersecurity and Infrastructure Security Agency (2016), 'Cyber-Attack Against Ukrainian Critical Infrastructure', ICS Alert IR-ALERT-H-16-056-01, 25 February 2016, https://www.cisa.gov/news-events/ics-alerts/ir-alert-h-16-056-01.

armed conflict, as recognized by the United Nations General Assembly.[12] Concentrating on Russian-linked proxies allows for a coherent analytical lens on questions of accountability, state responsibility and the integration of cyber capabilities within an offensive war strategy.

At the same time, many states other than Russia increasingly work with non-state actors for cyber defence in conflict situations, though the nature and implications of these relationships differ significantly from the malicious proxy activities examined in this paper. Commercial entities such as Microsoft and Starlink have provided defensive resources and capabilities for Ukraine, while volunteer organizations like the IT Army of Ukraine and various hacktivist groups have conducted operations in support of Ukraine's defence.

These actors – which range from major corporations to decentralized volunteer networks – illustrate the complex interplay between state, corporate and grassroots actors in modern conflict. Although these cases are not examined in depth, the paper acknowledges that such participation raises important questions, particularly regarding the boundaries between defensive and offensive action and the consequences – including under international humanitarian law (IHL) – of increasing civilian and corporate involvement in hostilities.

Thirdly, this paper builds on the operational picture to examine an increasingly urgent policy question: how to hold cyber proxies conducting malicious operations accountable in a conflict environment where responsibility is intentionally blurred. Existing scholarship highlights substantial barriers to accountability – these include opaque state–proxy relationships, inconsistent public attribution of cyber operations to specific state or non-state actors, and the difficulties of establishing legally meaningful links between states and non-state actors.[13] The barriers are compounded by the structural fragmentation of response mechanisms. Different states employ different attribution standards; sanctions regimes often operate independently from criminal prosecutions; and technical evidence produced by private firms has historically translated inconsistently into coordinated policy action, although this is gradually improving. Diplomatic responses can also proceed on separate tracks from operational disruption efforts.

This fragmentation is not merely an administrative inconvenience; it fundamentally limits the ability of states and international partners to deter or constrain malicious cyber actors, thus leaving exploitable gaps that adversaries systematically leverage. Addressing these challenges, we argue, requires a multidimensional framework capable of reflecting both the operational complexity of proxy activity and the spectrum of tools available to states.

Accordingly, this paper frames accountability as consisting of two dimensions: 'disruption' and 'cost imposition'. In the cyber proxy context, we argue, accountability is achieved by deploying these mutually reinforcing sets of instruments in service of a single strategic objective, **'deterrence'**:

---

12 United Nations General Assembly (2022), 'Aggression against Ukraine', Resolution ES-11/1, 2 March 2022, https://undocs.org/A/RES/ES-11/1.
13 For example, Finnemore, M. and Hollis, D. B. (2020), 'Beyond Naming and Shaming: Accusations and International Law in Cybersecurity', *European Journal of International Law*, 31(3), pp. 969–1003, https://doi.org/10.1093/ejil/chaa056.

— **Disruption**: this term refers to operational measures designed to degrade proxy capabilities in real time and limit the ability of proxies to conduct ongoing or imminent attacks.

— **Cost imposition**: this refers to legal, financial and reputational measures that increase the cost of hostile activity and constrain cyber proxies' future operations.

To be effective, deterrence must establish predictable consequences and behavioural expectations that shape adversaries' decision-making and influence their calculus around future operations when disruption and cost-imposing measures are credibly applied and communicated.

Critically, disruption and cost imposition must function as integrated components of a strategically coherent response rather than as parallel, uncoordinated tracks. Strategic coherence means that disruption and cost imposition are aligned across criminal, diplomatic and operational contexts – and that both consistently serve the overarching objective of deterrence. Achieving this integration in policy and operational practice is essential for developing effective responses to state-aligned cyber proxies, both in the Ukrainian conflict and in potential future theatres where such actors will almost certainly play a significant role.

The rest of this paper is structured as follows. Chapter 2 maps Russia's cyber proxy ecosystem, outlining definitional approaches, our analytical framework and the impact of proxies' activities. Chapter 3 assesses the effectiveness of international legal and policy frameworks, including the Framework for Responsible State Behaviour in Cyberspace, for addressing proxy activity. This chapter analyses, in particular, the various rules of international law relevant to the activities of proxies. Chapter 4 evaluates the disruption and cost imposition measures and tactics that have been employed by Ukraine and its allies, and assesses the impact these have had on deterring hostile Russian cyber operations. Chapter 5 presents policy recommendations organized around the imperative of building strategic coherence, and advocates a three-tiered response hierarchy comprising what we term 'core levers', 'amplifiers' and long-term 'enablers'; it is followed by a brief concluding chapter.

This research was informed by a combination of literature review; semi-structured interviews with legal, cyber and Russia experts; and an expert roundtable, held at Chatham House in November 2025, that focused on the different potential pathways for holding cyber proxies accountable. Insights from these sources have guided our analytical framework, validated our operational and legal observations, and helped shape the dual approach to accountability (disruption and cost imposition) outlined in this paper.

02
Mapping Russia's cyber proxy ecosystem

Russian cyber proxies exist in a complex and crowded operational landscape, in which multiple actors often overlap. This messiness and seeming disorder are advantageous for Russia – increasing disruption, creating confusion about the identities of perpetrators, and complicating accountability mechanisms.

While this paper focuses on Russian cyber proxies in the context of the war in Ukraine, the broader problem is systemic: states now routinely deploy proxy actors across multiple domains and regions – cyber, sabotage, influence operations, paramilitary activities and informational warfare. In the case of Russia's hybrid war against Europe, proxies constitute a central instrument of strategic competition and coercion.[14] The use of non-state and semi-state actors enables Russia to sustain pressure, cause disruption and operate below the threshold of conventional war – while preserving plausible deniability. Russia uses many different tools – from disinformation campaigns to sabotage and cyberattacks – but the underlying logic of proxy use is the same: operators are shielded behind a façade of non-state status, complicating accountability and response.

Critically, we argue, while the specific measures appropriate for responding to each type of proxy activity (cyberwarfare, physical sabotage, information operations, etc.) may vary by context, the need for strategic coherence remains constant across domains. Recognizing proxy actors as a structural challenge

14 Jones, S. (2025), 'Russia's hybrid warfare puts Europe to the test', *Financial Times*, 9 December 2025, https://www.ft.com/content/2084e87d-d491-4852-8449-f90b73d4788b.

to international security therefore demands not merely ad hoc or domain-specific responses, but also a holistic enforcement framework that coordinates tools for both disruption and cost imposition.

Approaches to defining cyber proxies

Any attempt to map Russia's cyber proxy ecosystem must begin by recognizing that the term 'cyber proxy' has no universally accepted definition. Cyber proxies operate in a dispersed digital space, often across borders, and with deliberate obfuscation both by states and by non-state actors.[15] This makes their relationships with sponsoring states more fluid and harder to observe, and makes it hard to establish accountability for malign cyber operations. Russia's cyber proxy ecosystem, in particular, spans military intelligence units, criminal syndicates, front companies, patriotic hackers and loosely organized hacktivists. Many of these actors shift roles or identities over time. As a result, mapping cyber proxies and their networks is inherently challenging, and never a static exercise.

Despite these difficulties, understanding the cyber proxy ecosystem is critical. The purpose of mapping is not simply to list actors, but to understand patterns of alignment and how actors work together across a broad landscape, even if it is not possible to develop a full picture. Doing so helps clarify where Russia relies on state-directed units, where it exploits permissive environments, and where opportunistic actors generate effects that align (whether intentionally or incidentally) with Russian strategic interests. Mapping the cyber proxy ecosystem also highlights how attributional uncertainty, deniability and the diffusion of cyber capabilities create policy and legal challenges for states seeking to respond.

Existing literature offers several approaches to defining cyber proxies. Notable approaches include Andrew Mumford's understanding of proxies as non-state actors leveraged by states to advance political or military objectives while maintaining plausible deniability;[16] and Tim Maurer's adaption of this concept to cyberspace, emphasizing a spectrum of state influence.[17] By starting from a broad definition, 'actor B acting for actor A', Maurer formalizes the proxy relationship while leaving room for variations in autonomy and operational control. His conceptualization is integral to the analysis in this paper.

Since 2016, the cyber proxy phenomenon has grown substantially. In the mid-2010s, only a limited number of states – most prominently Russia, Iran and, to a lesser extent, China – had begun employing non-state actors to conduct cyber operations as a means of achieving political goals without assuming full responsibility for the consequences.[18] A decade later, the landscape has changed significantly even beyond the Russian context. China's cyber ecosystem, little more than an informal network of hacker collectives in the mid-1990s and 2000s, has

15 When discussing cyber proxies, this paper refers exclusively to non-state actors and does not include technical infrastructure or automated systems that can be remotely exploited.
16 Mumford, A. (2013), 'Proxy warfare and the future of conflict', *RUSI Journal*, 158(2), pp. 40–46.
17 Maurer, T. (2018), *Cyber Mercenaries: The State, Hackers, and Power*, Cambridge: Cambridge University Press.
18 Ibid.

evolved greatly in the intervening years to become a flourishing web of overlapping actors in which cyber proxies are core enablers of the state.[19] As several participants at our November 2025 workshop emphasized, proxies are no longer marginal or exceptional actors. They are now deeply embedded in the normal operating environment of cyber conflict. Russia's war against Ukraine has made this shift especially visible. Russia's proxy actors operate as part of a broader ecosystem that blends cyber disruption, information operations and strategic signalling. Their role is not peripheral but central to how Russia conducts hostile activity below the threshold of armed attack.

Given these developments, and operational realities in cyberspace (including the difficulty of attribution, fluid group identities, and the alignment of non-state actors with state objectives), there is a need for flexible, empirically informed definitions on the part of organizations mapping these spaces.

Organizations that monitor and provide intelligence on cyber threats generally adopt an operational or behavioural approach to defining cyber proxies. Google's Threat Analysis Group, Microsoft and Recorded Future all classify potential proxies by observable indicators of alignment, such as target selection, timing, infrastructure overlap, shared tooling, public statements of political motive or responsiveness to a given state's strategic priorities.[20] These approaches intentionally avoid claiming firm command-and-control relationships between a state-level sponsor and a specific proxy unless the evidence is overwhelming. Instead, they rely on confidence levels to describe the existence of probable state links, recognizing that cyber operations often involve partial visibility or deliberate obfuscation. For example, when a hacker group claims responsibility for an attack that the group did not perpetrate, this may be a deliberate attempt to mislead targets or investigating organizations.

To establish a practical and analytically sound definition of cyber proxies, this paper maps them across a range of relationship types – from APT-commissioned actors operating under close state direction, through criminal and hacktivist groups enjoying varying degrees of state tolerance, to commercial enablers with no direct state relationship. This analytical framework has significant implications for how accountability mechanisms are designed and applied, as different relationship types require different policy responses.

---

19 Royal United Services Institute (2025), '40 red hackers who shaped China's cyber ecosystem', 9 December 2025, https://www.rusi.org/explore-our-research/publications/commentary/40-red-hackers-who-shaped-chinas-cyber-ecosystem.
20 Google Threat Analysis Group (2023), *Fog of war: How the Ukraine conflict transformed the cyber threat landscape*; Microsoft Threat Intelligence (2022), *Defending Ukraine: Early lessons from the cyber war*; Recorded Future (2022), *Russian cyber operations and the criminal ecosystem*.

Building on these strands of scholarship, and recognizing the need for a definition broad enough to capture both a range of actors and a range of potential levels of state involvement, this paper defines cyber proxies as follows:

> Cyber proxies are non-state actors that engage in malicious cyber operations under varying degrees of state direction, sponsorship or alignment.

Russian cyber proxies: the current landscape

Any consideration of Russian cyber proxy usage must necessarily situate cyber proxies within the context of Russia's broader information security ecosystem. This is a landscape in which cyber operations, information control, propaganda, disinformation and media manipulation are not discrete domains but deeply intertwined components of state strategy. For Russia, 'information confrontation' is an umbrella concept that combines many different strands – such as technical cyber operations, psychological operations, propaganda, censorship, intelligence gathering and influence campaigns – into a single strategic domain.[21]

Russia's broader information security ecosystem is a landscape in which cyber operations, information control, propaganda, disinformation and media manipulation are not discrete domains but deeply intertwined components of state strategy.

Russia's concept of information confrontation is described as 'a form of conflict between parties … each of which attempts to cause the other defeat or damage by means of information impact … [it has become] a form of combat in which information is both the tool, the environment, and the target'.[22] Evidently, this 'environment', as Keir Giles argues, goes well beyond cyberspace; the definition includes public opinion and narratives. Scholars such as Timothy Thomas have long argued that Russian military thinkers conceive of information conflict as occupying a holistic battlespace in which psychological, political and cyber tools reinforce one another and can be deployed in parallel during peace and wartime.[23] As a result, cyber proxies cannot be analysed only as technical disruptors. They are embedded within a much broader Russian strategy aimed at shaping perceptions, generating ambiguity and eroding adversaries' ability to respond.

---

21 Thomas, T. L. (2016), 'Russia's information warfare strategy: Can the nation cope in future conflicts?', *Journal of Slavic Military Studies*, 27(1), pp. 101–30.
22 Giles, K. (2023), *Russian cyber and information warfare in practice: Lessons observed from the war on Ukraine*, Research Paper, London: Royal Institute of International Affairs, https://www.chathamhouse.org/2023/12/russian-cyber-and-information-warfare-practice.
23 Scholars like Timothy Thomas have long argued that Russian military thinkers conceive of information conflict as occupying a holistic battlespace in which psychological, political and cyber tools reinforce one another and can be deployed in parallel during peace and wartime. See Thomas (2016), 'Russia's information warfare strategy'.

Russia's approach to information confrontation is associated with a tightly managed domestic media environment, the use of online propaganda and troll networks, and disinformation and cyber activities.[24] This paper recognizes the intertwined relationship between cyber operations and influence operations, acknowledging that both are products of a closely controlled Russian information ecosystem. Our analysis focuses on cyber proxies because they raise distinct and consequential questions around attribution, state responsibility and legal accountability. Proxies are where the opacity of the Russian information ecosystem creates the greatest policy challenges; isolating this element enables more precise analysis and more actionable recommendations.

Challenges in mapping the Russian cyber proxy ecosystem

The proliferation of Russian proxy actors, as well as the fluidity of these actors across ambiguous spaces, makes mapping Russia's cyber proxy ecosystem a complex task. There are four primary challenges.

Firstly, proxy relationships in cyberspace **resist simple categorization**. Russian cyber operations draw both on direct state actors – such as Sandworm and other GRU-integrated units – and on a range of non-state proxies, from APT-commissioned actors operating under close state direction, through criminal groups and hacktivist networks operating with varying degrees of state tolerance, to commercial enablers with no direct state relationship. Actors may shift between categories depending on the operation, target or geopolitical context, and some may occupy different positions simultaneously.

The second challenge is that **this ecosystem is not static**. Groups rebrand, splinter, merge and adopt new identities, sometimes to obscure attribution, sometimes to signal new alliances, sometimes due to disruptive action taken against them or even internal disagreement between members, and sometimes simply to maintain relevance in a competitive underground economy. Campaign names evolve, and similar tools may be used by multiple actors with varying degrees of skill. Opportunistic actors may suddenly attach themselves to a Russian narrative following major battlefield events, while previously active collectives may fade or reappear under new banners. This dynamism limits the value of static taxonomies and requires continuous assessment.

Thirdly, **different groups often occupy overlapping categories and perform hybrid functions**. Criminal groups may undertake profit-motivated ransomware campaigns alongside politically motivated disruptions (with often only the latter aligned with Russian state interests). Hacktivist collectives sometimes perform primarily informational or psychological functions, such as defacing websites, leaking stolen data or amplifying narratives through Telegram, but they may also participate in low-level disruptive operations themselves. State-backed APTs may

24 Mullaney, S. (2022), 'Everything flows: Russian information warfare forms and tactics in Ukraine and the US between 2014 and 2020', *The Cyber Defense Review*, 7(4), pp. 193–212, https://www.jstor.org/stable/48703300.

outsource components of campaigns to criminal subcontractors or rely on tolerant ecosystems to 'launder infrastructure'.[25] The result is a blurring of motivations, methods and organizational roles, making categorization inherently approximate.

Finally, **many incidents remain undisclosed or only partially observable in the public domain**. Open-source reporting, public attribution and media coverage capture only a fraction of activity, meaning that the proxy ecosystem is likely far denser and more active than publicly documented. As a result, analyses based solely on open-source information may underestimate both the frequency and strategic impact of cyber operations. This limitation underscores the importance of continuous monitoring and integration of multiple intelligence sources to build a more accurate operational picture.

To understand Russia's cyber campaign against Ukraine, and the role that proxies have played, it is necessary to map the landscape of actors involved, examining both their organizational profiles and their relationships with the Russian state. Yet in light of the above, mapping proxies is less about fixing actors into permanent boxes and more about assessing patterns of alignment, behaviour and utility across an evolving ecosystem. Attribution in cyberspace remains complex, particularly where self-proclaimed 'patriotic' groups or criminal entities are concerned, and available open-source evidence often reveals alignment with state objectives rather than direct evidence of state tasking.

Classification of Russian cyber proxies

Table 1 categorizes Russian cyber proxies according to their relationship with the Russian state, primary activities and degree of strategic intent. The categories reflect variable and overlapping degrees of state control and alignment, as mentioned ranging from APT-commissioned proxies under direct intelligence guidance to commercial enablers – hosting providers, cryptocurrency services and IT contractors – whose relationship with the state is indirect, willingly providing services to malicious actors rather than acting under state direction. The framework should not be read as implying a neat linear sequence: ideological hacktivists, though largely self-directed, occupy an intermediate position because their operations have generally produced effects aligned with Russian state objectives and have been amplified through state-linked media channels. Influence operation actors cut across the typology entirely. This typology draws on observable patterns in Russian-linked cyber activity since 2022, though many proxy relationships predate the full-scale invasion.

25 This is the practice whereby state-backed APTs deliberately route their operations through infrastructure associated with criminal actors or permissive environments, such as rented servers or botnets, as a means of obscuring links to the state, complicating attribution and reusing infrastructure.

Table 1. Typology of actors within Russia's cyber proxy ecosystem

Category	Characteristics	Examples	State relationship	Primary operations	Operational intent
APT-commissioned proxies	Non-state actors formally or semi-formally tasked, sponsored or guided by Russian intelligence. Such actors retain partial operational autonomy and execute tasks aligned with state objectives, but may have discretion over timing, methods or tools.	Hacktivist collectives occasionally guided for specific campaigns; semi-autonomous contractors temporarily commissioned for cyber operations.	**High to medium control:** proxies receive direct or indirect guidance from intelligence agencies, and maintain some discretion over execution.	Targeted intrusions, wiper attacks, DDoS campaigns, tactical disruption.	**Strategic:** provide deniable cyber capabilities, support military/political objectives, and amplify state reach while maintaining plausible deniability.
State-tolerated criminal groups	Cybercriminals and ransomware operators. Such groups avoid Russian or Russia-allied targets. Primary motivations are financial but can align with Russian state objectives opportunistically.	Conti, TrickBot, Wizard Spider, Revil, LockBit.[26]	**Medium control:** tacitly tolerated, may align with state during conflict, occasionally influenced by intelligence signals.	Ransomware, data exfiltration, opportunistic disruption.	**Dual-purpose:** financial gain plus opportunistic strategic disruption, may support state interests without formal tasking.
Mercenary/ contractor groups	Private cyber operators providing bespoke offensive capabilities; hired for specific targets; operate for profit but may be strategically aligned with Russian state.	Contractors associated with private military companies, commercial offensive cyber firms.	**Medium control:** transactional relationships with Russian intelligence services; operate for profit but aligned with Russian strategic objectives.	Custom malware, targeted intrusions, reconnaissance.	**Transactional and strategic:** provide surge capacity and specialized skills, and deniability for sensitive operations; profit-driven but strategically aligned with Russian state.
Ideologically aligned hacktivists	Volunteer or semi-organized groups supporting Kremlin narratives; generally limited technical sophistication; visibility boosted by state media and Telegram channels.	KillNet,[27] XakNet,[28] NoName057(16),[29] CyberArmyofRussia_Reborn.[30]	**Low to medium control:** tacit encouragement and narrative amplification; primarily self-directed.	DDoS attacks, website defacement, low-sophistication disruptions, information operations, psychological warfare.	**Performative and disruptive:** reinforce narratives, degrade morale, signal Russian cyber capabilities.

26 Microsoft Threat Intelligence (2022), *Defending Ukraine: Early lessons from the cyber war*; Recorded Future (2023), *Dark Covenant 2.0: Cybercrime, the Russian State, and the War in Ukraine*, https://www.recordedfuture.com/research/dark-covenant-2-cybercrime-russian-state-war-ukraine.
27 Mandiant Intelligence (2022), 'Hacktivists Collaborate with GRU-sponsored APT28', 23 September 2022, https://cloud.google.com/blog/topics/threat-intelligence/gru-rise-telegram-minions.
28 Ibid.
29 European Union Agency for Criminal Justice Cooperation (2025), 'Hacktivist group responsible for cyberattacks on critical infrastructure in Europe taken down', press release, 16 July 2025, https://www.eurojust.europa.eu/news/hacktivist-group-responsible-cyberattacks-critical-infrastructure-europe-taken-down; U.S. Department of Justice (2025), 'Justice Department Announces Actions to Combat Two Russian State-Sponsored Cyber Criminal Hacking Groups', press release, 9 December 2025, https://www.justice.gov/opa/pr/justice-department-announces-actions-combat-two-russian-state-sponsored-cyber-criminal.
30 U.S. Department of Justice (2025), 'Justice Department Announces Actions to Combat Two Russian State-Sponsored Cyber Criminal Hacking Groups'.

Category	Characteristics	Examples	State relationship	Primary operations	Operational intent
Dual-use/ commercial actors*	Private companies and contractors that knowingly provide dual-use services to malicious actors, motivated by profit or ideological alignment.	Russian hosting providers (using, for example, so-called 'bulletproof hosting' services), VPN services, IT contractors providing custom tools.	**Willing collaboration:** provide services knowingly, often with plausible deniability.	Infrastructure hosting, tool development, obfuscation services, money laundering (crypto), logistical support.	**Enabling:** provide essential infrastructure for proxy operations; financially or ideologically motivated.
Influence operation actors (cross-cutting)	Actors shaping narratives, coordinating hack-and-leak campaigns, amplifying cyber operations. Activities include coordinated leaks, messaging through Telegram channels, doxing and reputational attacks.	APT-linked leak operations, coordinated use of Telegram channels, CyberArmyofRussia_Reborn.[31]	**Cross-spectrum:** state-directed, state-aligned or opportunistic; overlaps with technical intrusion groups.	Hack-and-leak operations, doxing, mass harassment, propaganda amplification.	**Strategic:** shape information environments, amplify psychological effects of cyber incidents, erode trust, create political pressure, generate ambient effects at low cost.

* This category excludes infrastructure that is coerced or unwittingly exploited (e.g. compromised servers, hosting providers under regulatory duress). While such infrastructure enables proxy operations, it lacks the willing engagement or alignment that fits our definition of proxy relationships.
Additional sources: Microsoft Threat Intelligence (2022), *Defending Ukraine: Early lessons from the cyber war;* Google Threat Analysis Group (2023), *Fog of war: How the Ukraine conflict transformed the cyber threat landscape*; Recorded Future (2022), *Russian cyber operations and the criminal ecosystem*; Axon, L. et al. (2024), 'Private-public initiatives for cybersecurity: the case of Ukraine', *Journal of Cyber Policy*, 9(3), pp. 399–422, https://doi.org/10.1080/23738871.2025.2451256.

Key proxy cyber operations, 2022–24

Table 2 highlights a selection of significant Russian proxy cyber operations that targeted Ukraine and its allies between 2022 and 2024. The focus here is on the variety and density of the Russian proxy ecosystem active during this period. These operations span multiple proxy categories from Table 1, and range from politically motivated ransomware campaigns and coordinated DDoS attacks to information and influence operations on platforms such as Telegram and across cloned media websites.

The hybrid nature of these attacks reflects how different proxy actors often coordinate, opportunistically align or amplify each other's efforts, generating larger-scale effects than would be possible individually.

Taken together, these examples illustrate that Russia's cyber activity extends far beyond Ukrainian territory. Proxy actors have routinely targeted Ukraine's closest supporters in Europe and North America. This demonstrates both

31 Recorded Future (2023), *Dark Covenant 3.0: Controlled Impunity and Russia's Cybercriminals*, https://www.recordedfuture.com/research/dark-covenant-3-controlled-impunity-and-russias-cybercriminals; and Giles (2023), *Russian cyber and information warfare in practice*.

the external-facing nature of Russia's proxy ecosystem and the deliberate use of deniable, multi-modal actors to generate pressure and shape political narratives across the West.

It is important to note that while Table 2 highlights a selection of high-impact proxy operations, it contains only incidents that have been publicly reported. Many attacks and campaigns likely remain undisclosed or only partially visible to outside observers, meaning that the true scale, intensity and complexity of Russia's proxy ecosystem exceed what can be captured here.

Table 2. Selected Russian cyber proxy operations against Ukraine and allied targets (2022–24)

Operation and date	Targets	Suspected perpetrator (if known)	Further details	Impact
Somnia ransomware attacks, late 2022[32]	Ukrainian defence-linked organizations, logistics companies, state agencies	From Russia With Love (FRwL)	FRwL is reported to have used fake 'Advanced IP Scanner' installers to drop the Vidar stealer malware into target systems and networks and deploy Somnia ransomware, aimed at disruption rather than ransom; CERT Ukraine tracked multiple attacks across 2022.[33]	Operational disruption of defence logistics; demonstrated criminal-ideological hybrid tactics.
KillNet DDoS campaigns, 2022–24[34]	NATO structures, US and EU government websites, European Investment Bank, Western websites	KillNet	Waves of politically motivated DDoS campaigns[35] in response to weapons support for Ukraine; targeted public institutions and services.	Temporary service outages; widened conflict to NATO allies; low-cost, high-visibility operations.
Doppelgänger disinformation campaign, 2022–24[36]	European public opinion and political discourse (France, Germany, UK, Poland, EU)	Cluster of bot/troll networks and aligned contractors	Cloned news websites impersonating major outlets disseminated fabricated anti-Ukraine narratives, amplified via social and messaging platforms.	Eroded trust in media; amplified anti-Ukraine narratives; prompted platform takedowns and government warnings.

32 Constantinescu, V. (2022), 'Russian Hacktivists Infect Ukrainian Targets with New Somnia Ransomware', Bitdefender, 15 November 2022, https://www.bitdefender.com/en-us/blog/hotforsecurity/russian-hacktivists-infect-ukrainian-targets-with-new-somnia-ransomware.
33 Ibid.; and CERT-UA (2022), 'Cyberattacks Using Fake Advanced IP Scanner Installers', Computer Emergency Response Team of Ukraine, https://cert.gov.ua/article/2724253.
34 White Blue Ocean (2022), 'Killnet: The Pro-Russia Threat Group Targeting Western Countries', 16 October 2022, https://www.whiteblueocean.com/newsroom/killnet-the-pro-russia-threat-group-targeting-western-countries.
35 Mandiant Intelligence (2022), 'Hacktivists Collaborate with GRU-sponsored APT28'.
36 EU DisinfoLab (2022), 'Doppelganger', investigation hub, first published September 2022, https://www.disinfo.eu/doppelganger (accessed 23 Feb. 2026).

Operation and date	Targets	Suspected perpetrator (if known)	Further details	Impact
NoName057(16) DDoS campaigns, 2022–24[37]	Western government services, EU critical infrastructure, NATO sites	NoName057(16)	Coordinated DDoS attacks timed to announcements of sanctions or military aid; targeted national portals and critical services in multiple countries.[38]	Government portal disruptions: rapid-response signalling coordinated with Russian diplomatic/ military events.
XakNet hack-and-leak operations, 2022–23[39]	Ukrainian government and military agencies	XakNet	Alleged to have conducted intrusions, stolen sensitive data and released data via Telegram and state-adjacent media; blended cyber intrusion with information operations.[40]	Leaking of sensitive data; psychological pressure on Ukrainian officials; amplification of Russian information operations.

Impact of proxies

In considering the role cyber proxies have played for Russia in its war against Ukraine, it is necessary to separate different types of impact which may be felt at different times. While organizational impact may manifest itself immediately, tactical, operational and even strategic impacts may emerge more slowly. Assessing cyber proxies' impacts is thus a multi-pronged task.

Tactical impacts. Proxies caused nuisance and created targeted disruption through low- to medium-sophistication operations. DDoS and website defacement campaigns degraded service availability and imposed mitigation costs on Ukrainian and allied organizations. KillNet and affiliated collectives targeted government websites, hospitals and airport infrastructure across Germany, Lithuania, Poland and the UK. These attacks forced their targets to implement costly defensive measures, and signalled to Western publics that supporting Ukraine carried direct cyber consequences.

Operational impacts. Higher-end proxy activity – politically aligned ransomware, hack-and-leak operations, sophisticated DDoS campaigns – produced more serious consequences when targeting critical infrastructure or information networks.

37 Recorded Future Insikt Group (2025), 'Inside DDoSia: NoName057(16)'s Pro-Russian DDoS Campaign Infrastructure', Recorded Future, July 2025, https://www.recordedfuture.com/research/anatomy-of-ddosia.
38 European Union Agency for Criminal Justice Cooperation (2025), 'Hacktivist group responsible for cyberattacks on critical infrastructure in Europe taken down'.
39 Canadian Centre for Cyber Security (2023), *Cyber threat activity associated with the Russian invasion of Ukraine*, https://www.cyber.gc.ca/sites/default/files/cyber-threat-activity-associated-russian-invasion-ukraine-e.pdf.
40 Mandiant Intelligence (2022), 'Hacktivists Collaborate with GRU-sponsored APT28'.

The Somnia ransomware attack by FRwL and hack-and-leak operations by XakNet disrupted communications, stole data, and created operational friction not only in Ukraine but also among European partners reliant on shared digital infrastructure. Waves of DDoS attacks against European election bodies, parliaments and ministries by KillNet and NoName057(16) were designed to create political pressure, destabilize institutional processes such as electoral administration and public communications, and force the diversion of resources.

Impacts have been significantly mitigated by Ukraine's strong cyber resilience, built through years of preparation, operational experience and deep public–private partnerships.

Strategic impacts. Cyber operations contributed to influence operations and narrative shaping beyond Ukraine's borders. Influence campaigns such as Doppelgänger combined networked hack-and-leak activity with fabricated media outlets to amplify anti-Ukraine narratives across Europe. The cumulative effect was a degradation of morale, the diversion of defensive resources and the shaping of international perceptions regarding the importance of cyber power and resilience.

Mitigation and resilience

These impacts have been mitigated by Ukraine's strong cyber resilience, built through years of preparation, operational experience and deep public–private partnerships. Sustained cooperation with allied governments and private sector actors helped contain and remediate attacks quickly. However, the involvement of the private sector in conflict-related cyber defence cannot be taken for granted. As conflicts endure, the costliness of providing tech services will be significant, for example as public outrage subsides and as commercial interests and financial affordability considerations may come into play.[41] Furthermore, the risk that civilian staff could be identified as combatants may make private companies increasingly reluctant to participate in conflict. It is thus crucial to consider the role of cyber proxies and cyberattacks not only in Ukraine, but also where they might play a part in other conflicts where public–private partnerships may be absent, or where states' preparedness and resilience are lower.

41 Axon, L. et al. (2024), 'Private-public initiatives for cybersecurity: the case of Ukraine', *Journal of Cyber Policy*, 9(3), pp. 399–422, https://doi.org/10.1080/23738871.2025.2451256.

03 International legal and policy frameworks relevant to cyber proxy activity

The activities of cyber proxies engage various rules of international law, as well as being covered by some soft law and policy initiatives. While the threshold for attributing the behaviour of a proxy to a state is not easily met, some rules bind proxies directly as individuals.

This chapter considers the extent to which existing international and policy frameworks in relation to malicious cyber activity can help hold cyber proxies to account. While the chapter focuses on Russia's use of proxies in its war on Ukraine, our analysis has broader relevance to any state that seeks to work (to whatever degree of proximity) with non-state actors – including ideologically aligned hacktivists or commercial entities – to carry out cyber operations in order to further state goals.

Multilateral diplomacy

UN discussions, particularly those within the Framework for Responsible State Behaviour in Cyberspace, have repeatedly affirmed that malicious cyber operations – including those conducted through proxies – undermine international peace and security. Such discussions also emphasize that states should not exploit non-state actors for malicious cyber operations.[42] The application of aspects of the Framework for Responsible State Behaviour established in discussions in the UN's First Committee over the past 20 years, particularly on norms and international law, is examined later in this chapter.

Regulation in this area needs updating to recognize the increasing role of private military and security companies in cyber activity, both offensive and defensive.

As Table 1 above illustrates, one form of cyber proxy activity in the Russia–Ukraine context is the practice of mercenary or contractor groups providing bespoke offensive capabilities for profit, in alignment with Russian strategic objectives. There is some international governance of private military and security companies (PMSCs). For example, the *Montreux Document*, a 2008 joint initiative by the Swiss government and the International Committee of the Red Cross (ICRC), affirms states' obligations under international law, particularly IHL and international human rights law, in relation to PMSCs.[43]

Regulation in this area needs updating to recognize the increasing role of PMSCs in cyber activity, both offensive and defensive.[44] There are some efforts under way to do so. For example, a UN Working Group on the Use of Mercenaries, which operates under the auspices of the UN Human Rights Council, has been working on a draft convention on the regulation, monitoring and oversight of PMSCs' activities. The definition of PMSCs in the latest draft includes contractors providing services 'whether on land, in the air or at sea, or whether in cyberspace or outer space'.[45] While the draft seeks to strengthen states' governance of PMSCs, including by requiring the integration of standards on international human

---

42 For example, as early as 2013, the UN Group of Government Experts affirmed that 'States must not use proxies to commit internationally wrongful acts' in its Report to the UN General Assembly of 24 June 2013, UN Doc A/68/98, https://docs.un.org/en/a/68/98.

43 Swiss Federal Department of Foreign Affairs and International Committee of the Red Cross (2008), *The Montreux Document: On pertinent international legal obligations and good practices for States related to operations of private military and security companies during armed conflict*, https://www.montreuxdocument.org/about/montreux-document.html.

44 See Bernard, V. (2025), 'Symposium on PMSCs: Revising the International Regulation of Private Military and Security Companies in the Digital Age', *Opinio Juris,* 16 July 2025, https://opiniojuris.org/2025/07/16/symposium-on-pmscs-revisiting-the-international-regulation-of-private-military-and-security-companies-in-the-digital-age.

45 UN Working Group on PMSCs (2025), 'Revised Fourth Draft Instrument on an International Regulatory Framework on the Regulation, Monitoring of and Oversight over the Activities of Private Military and Security Companies', 5 March 2025, https://www.ohchr.org/sites/default/files/documents/hrbodies/hrcouncil/igwg-military/session6/IGWG-PMSCs-Revised-fourth-draft-PMSCs-clean-version-copy.pdf.

rights law, due diligence and training, the prospect of a binding instrument in this area is still some way off (and even if it were to materialize, it is questionable whether Russia would become party to it).

Voluntary industry initiatives seek to complement these multilateral efforts. For example, the Cybersecurity Tech Accord, signed by over 160 private companies operating in the cyber sector, aims to promote responsible behaviour in cyberspace, including curbing the proliferation of cyber mercenaries.[46] This includes support for the Paris Call Blueprint on Taming the Cyber Mercenary Market, published in 2023, which contains proposals to address the escalating challenge of cyber mercenaries.[47] The Pall Mall Process seeks to tackle the proliferation and irresponsible use of commercial cyber capabilities.[48] While adoption and enforcement remain uneven, these frameworks provide reputational pressure and legal hooks where state action alone is insufficient.

International law

As part of the Framework for Responsible State Behaviour in Cyberspace mentioned above, states have agreed that international law applies in the cyber context.[49] Various areas of international law relevant to the activities of cyber proxies include the law of armed conflict; international criminal law; rules on attribution under the law on state responsibility; and the principle of due diligence.

As will be seen, there are important limitations to international law's ability to constrain and punish cyber proxies. In practice, it is often difficult to attribute the activities of cyber proxies to a state due to the high thresholds of control set out in the rules on state responsibility. At the same time, few rules of international law are directed at non-state actors. And as well as being state-centric, international law provides only limited means of enforcement. For this reason, the activities of proxies have been described as falling within, if not a legal black hole, a 'normative safe zone'.[50] This is, of course, one of the attractions for Russia of using cyber proxies.

---

46 Cybersecurity Tech Accord, https://cybertechaccord.org.
47 Paris Peace Forum (2023), 'Paris Call: Taming the Cyber Mercenary Market', 10 November 2023, https://parispeaceforum.org/publications/paris-call-taming-the-cyber-mercenary-market.
48 Foreign, Commonwealth and Development Office (2024), 'The Pall Mall Process: tackling the proliferation and irresponsible use of commercial cyber intrusion capabilities', 6 February 2024, https://www.gov.uk/government/publications/the-pall-mall-process-declaration-tackling-proliferation-and-irresponsible-use-of-commercial-cyber-intrusion-capabilities/the-pall-mall-process-tackling-the-proliferation-and-irresponsible-use-of-commercial-cyber-intrusion-capabilities.
49 See, for example, UN General Assembly (2013), 'Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security', Report of 24 June 2013, UN Doc A/68/98, paras 19–20, https://undocs.org/A/68/98 and Report of 22 July 2015, A/70/174, 22 July 2015, para 28(b), https://undocs.org/A/70/174.
50 Schmitt, M. and Vihul, L. (2014), 'Proxy Wars in Cyber Space: The Evolving International Law of Attribution', I(II) *Fletcher Security Law Review* 55–73, p. 72.

Understanding the law of armed conflict as it applies to proxies

Russia and Ukraine are in an international armed conflict, which is governed by international humanitarian law (IHL). States have agreed that the rules of IHL apply to cyberspace,[51] although debates are ongoing as to how those rules apply.[52] As discussed below, some IHL rules regulate how states should treat proxy actors, including requiring states to take responsibility for the actions of proxies in some circumstances. Some rules bind non-state actors as well as states. And cyber proxies participating in hostilities that disregard IHL risk being complicit in war crimes under international criminal law.[53]

The growing involvement of non-state actors such as citizen hackers in warfare raises a number of legal questions that are beyond the scope of this paper.[54]

The following sections provide a summary of how IHL applies to cyber proxies:

Regulating how states treat proxies

IHL does not prohibit participation in an armed conflict, but it does set out consequences that result from participation. In some situations, individuals acting in support of a state can be targeted by the armed forces of the other side, whether by cyber or other means. Cyber proxies such as hacker groups cannot be a party to an international armed conflict themselves, as they are not a state. However, in two situations, a proxy actor could qualify as a combatant under IHL, and thus would become targetable by the adversary. As a combatant, the proxy would also enjoy certain protections.

The first situation in which a proxy actor could qualify as a combatant is if **it is incorporated into a state's armed forces or meets the required organizational criteria.**[55] Military cyber units such as US Cyber Command or China's PLA Cyberspace Force would fall within their country's armed forces, and certain Russian APT groups have been attributed to military units of Russia's GRU intelligence agency.[56]

Cyber proxies that are not formally incorporated into the armed forces of a state could still be combatants if they are part of an organized group or unit under a responsible command. To qualify as an organized group, a proxy would need to have an internal hierarchical structure that ensures discipline within the group and that effectively subordinates the group, and renders it responsible,

---

51 See UN GGE (2021), 'Report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of Information Security', 14 July 2021, https://digitallibrary.un.org/record/3934214?ln=en&v=pdf; Rodenhäuser, T. (2025), 'The ICT resolution of the 34th International Conference: A first step towards protecting civilians in digitalizing armed conflicts', December 2025, https://rcrcconference.org/blog/the-ict-resolution-of-the-34th-international-conferencea-first-step-towards-protecting-civilians-in-digitalizing-armed-conflicts.
52 For views by a number of states and regional organizations in this area, see Cyber Law Toolkit: 'International humanitarian law (jus in bello)', https://cyberlaw.ccdcoe.org/wiki/International_humanitarian_law_(jus_in_bello).
53 ICC Office of the Prosecutor (2025), 'Policy on Cyber-Enabled Crimes under the Rome Statute', December 2025, https://www.icc-cpi.int/sites/default/files/2025-12/2025-cyber-eng.pdf.
54 For a detailed discussion, see Rodenhäuser, T. (2026), 'Civilian hackers in war: The limits that international humanitarian law imposes on volunteer IT armies, hacktivists and other civilian hackers', *International Review of the Red Cross*, I-39.
55 Article 43(1) of Additional Protocol I to the Geneva Conventions of 12 August 1949 and Relating to the Protection of Victims of International Armed Conflicts (Protocol I), 8 June 1977.
56 National Cyber Security Centre (2025), 'UK calls out Russian military intelligence for use of espionage tool', 18 July 2025, https://www.ncsc.gov.uk/news/uk-call-out-russian-military-intelligence-use-espionage-tool.

to a state party to the conflict. This is a high threshold that would not be met by groups organizing independently of a state or only through online open communication. Of the categories of proxy actor outlined in Table 1 above, most would not qualify as organized armed groups.

The second situation is if the proxy actors are not part of a state's armed forces or an organized group, so are considered civilians, but are **'directly participating in hostilities'**. Civilians enjoy protection against direct attack unless and for such time as they directly participate in hostilities.[57] For a proxy to qualify as directly participating in hostilities, its operations would have to meet three cumulative criteria: a threshold of harm; direct causation; and a belligerent nexus.[58]

In practice, these three criteria set a high threshold for a civilian to lose protection from attack – acts of cybercrime that directly cause harm (e.g. a ransomware operation) without a link to the conflict would not qualify. But where cyber proxies engage in offensive operations against enemy targets as an integral part of a cyber operation against military forces, they may be deemed to be directly participating in hostilities.[59] This could be the case, for example, if a civilian hacker deployed malware to disable a power grid and generate a blackout for the purpose of facilitating an attack by a state's armed forces, or used a smartphone app to provide tactical intelligence to attacking forces.[60] In doing so, the hacker would lose protection as a civilian and become exposed to targeting for as long as they were providing assistance to the armed forces.[61]

The legal framework that governs when civilians may lose their protected status and become legitimate military targets is complex; there is significant debate over what constitutes 'directly participating in hostilities' and for how long civilians who are doing so would be targetable.[62] Many states and commentators endorse the ICRC's 'revolving door' approach, under which civilians who engage in spontaneous, sporadic or unorganized direct participation in hostilities only lose their protection for the duration of the hostile act and regain their protected status once the act ends.[63] But some, particularly the US, adopt a broader approach, under which protection is only regained when there is 'affirmative disengagement' by the civilian from the hostile activity.[64] These issues are compounded in the cyber context, in which proxies can be constantly on and off their phones or computers, or cyber actors can deploy malware then walk away, with the malware continuing to operate without direct command – in both cases challenging traditional

---

57 Additional Protocol I to the Geneva Conventions, Art. 51(3).
58 For discussion of each criterion, see Melzer, N. (2009), 'Interpretative Guidance on the Notion of Direct Participation in Hostilities under International Humanitarian Law', p. 46. For a discussion of the application of these criteria in the cyber context, see Rodenhäuser (2026), 'Civilian hackers in war', pp. 27–31.
59 See Melzer (2009), 'Interpretative Guidance on the Notion of Direct Participation in Hostilities under International Humanitarian Law', for the ICRC's three cumulative conditions for an act to amount to direct participation in hostilities, p. 46.
60 See Schmitt, M. and Biggerstaff, C. (2022), 'Ukraine Symposium - Are Civilians Reporting with Cell Phones Directly Participating in Hostilities?', Articles of War, Lieber Institute for Law & Warfare, 2 November 2022, https://lieber.westpoint.edu/civilians-reporting-cell-phones-direct-participation-hostilities.
61 See Macak, K. (2023), 'Will the centre hold? Countering the erosion of the principle of distinction on the digital battlefield', *International Review of the Red Cross*, 105(923), pp. 980–81.
62 For a detailed exploration of the issues, see Hathaway, O., Pe'er, I. and Vera, C. (2025), 'Crowdsourced War' in *New York University Law Review*, Vol. 100, p. 1582 ff.
63 For the ICRC's approach, see Melzer (2009), 'Interpretative Guidance on the Notion of Direct Participation in Hostilities under International Humanitarian Law'.
64 U.S. Department of Defense, *Law of War Manual* 237, 5.8.4.2. See also Schmitt and Biggerstaff (2022), 'Ukraine Symposium - Are Civilians Reporting with Cell Phones Directly Participating in Hostilities?'.

temporal frameworks for determining when participation begins and ends.[65] Under IHL, in any circumstances where there is doubt about whether a person is a civilian or not, that person shall be considered a civilian.[66] If civilian cyber proxies are captured by an adversary, they may face prosecution under the domestic law of the adversary state.

State responsibility for proxies under IHL

States that are parties to an armed conflict are responsible for the conduct of any group operating under their instructions, direction or control.[67] There is debate about the meaning of 'direction or control'; generally, 'overall control' is considered sufficient in the IHL context.[68] Mere financing or equipping of hacker groups, or their activities, would not be sufficient. But a state would be responsible in situations in which it has a role in organizing the group's cyber operations or gives specific instructions to a hacker group regarding the commission of a particular cyber operation in violation of IHL, as may be the case for the first category listed in Table 1, which involves Russian APT groups commissioning cyber activity.[69] A case-by-case assessment will be required based on the facts.

States' responsibilities to make IHL known to proxies

Even when the tests of instruction, direction or control are not met, such that the state concerned is not internationally responsible for a proxy's conduct, all states have a due diligence obligation to ensure respect for IHL under Common Article 1 to the Geneva Conventions. This includes the obligation not to aid or assist in violations of IHL by others, nor to encourage private persons or groups to act in violation of IHL[70] – for example, by inciting civilian hackers to direct cyber operations against civilian objects such as hospitals. States also have an obligation to ensure that civilian populations under their authority respect IHL.[71] In the context of the conflict between Russia and Ukraine, both parties are under an obligation to make IHL rules known to civilian hackers and hacker groups, should demand that such actors respect IHL, and should take the measures necessary to suppress IHL violations.[72] Both parties are also obliged to search for, prosecute or extradite alleged perpetrators of grave breaches of IHL and to enact any necessary legislation in this respect. They are further required to suppress all other breaches of the Geneva Conventions.[73]

---

65 Hathaway, Pe'er and Vera (2025), 'Crowdsourced War', p. 1597.
66 Article 50 of Additional Protocol I.
67 ICRC (2016), 'Updated Commentary on the First Geneva Convention', paras 265–73, https://ihl-databases.icrc.org/en/ihl-treaties/gci-1949/introduction/commentary/2016.
68 See International Criminal Tribunal for the former Yugoslavia (ICTY), *Prosecutor v. Tadic* (Appeals Chamber), Jurisdiction, para 131.
69 See ICRC Report (2025), 'International Humanitarian Law and the Growing Involvement of Civilians in Cyber Operations and Other Digital Activities during Armed Conflict', p. 18.
70 Henckaerts, J.-M. and Doswald-Beck, L. (2025), *Customary International Humanitarian Law, Volume I: Rules*, Rule 144, https://www.icrc.org/sites/default/files/external/doc/en/assets/files/other/customary-international-humanitarian-law-i-icrc-eng.pdf.
71 See ICRC (2020), 'Commentary on the Third Geneva Convention', Article1, para 183, https://ihl-databases.icrc.org/en/ihl-treaties/gciii-1949/foreword/commentary/2020.
72 Article 1 of Third Geneva Convention; see also ICRC (2020), 'Commentary on the Third Geneva Convention', para 183 on Article 1.
73 ICRC (2020), 'Commentary on the Third Geneva Convention', para 184.

In practice, both Russia and Ukraine have encouraged civilians to participate in the hostilities using information and communication technologies (ICTs), for example as 'patriotic hackers'. As Table 2 makes clear, hacker groups such as Killnet have targeted civilian objects such as banks, medical facilities and civilian airports.[74] In doing so, the civilians participating in hostilities do not adhere to one of the fundamental tenets of IHL: protecting civilian objects from armed conflict.[75]

To raise awareness of the rules of IHL among civilian hackers, in 2023 advisers at the ICRC produced 'eight rules for civilian hackers during war and four obligations for states to restrain them'.

Some commentators have endorsed the notion that civilians should support the war effort and be 'responsibly irresponsible'.[76] But IHL embodies a careful balance between military necessity and humanity.[77] Civilian involvement in armed conflict risks generating confusion about who or what is a 'civilian', and increases the risk of erroneous or unlawful attacks.[78]

Obligations on both states and proxies

To raise awareness of the rules of IHL among civilian hackers, in 2023 advisers at the ICRC produced 'eight rules for civilian hackers during war and four obligations for states to restrain them'.[79] The purpose was to highlight rules that anyone who conducts a cyber operation in the context of armed conflict – whether a state or a non-state actor such as a civilian hacker or company – must respect. The document's provisions include a prohibition on the use of malware or other tools or techniques that spread automatically and damage military and civilian objects indiscriminately, and a rule not to conduct any cyber operation against medical and humanitarian facilities.

---

74 See, for example, Tidy, J. (2023), 'Meet the Hacker Armies on Ukraine's Cyber Front Line', BBC News, 15 April 2023, https://www.bbc.co.uk/news/technology-65250356. The article reports that Killnet called for and carried out disruptive attacks on hospital websites of Ukraine and its allies; see also the Killnet operations against Western allies listed in Table 2.
75 Under IHL, it is prohibited to attack civilian objects: Art. 52(1) AP I; this reflects customary international law. When a cyber operation constitutes an 'attack' under IHL is debated. It is widely accepted that cyber operations expected to cause death, injury or physical damage will do so, but there is debate about whether reasonably foreseeable indirect effects are included, and whether loss of computer functionality can constitute an attack. See Cyber Law Toolkit (undated), 'Attack (international humanitarian law)', https://cyberlaw.ccdcoe.org/wiki/Attack_(international_humanitarian_law).
76 Soesanto, S. and Gajos, W. (2025), 'Offensive Cyber Operations and Combat Effectiveness after Ukraine', Lawfare, 3 November 2025, https://www.lawfaremedia.org/article/offensive-cyber-operations-and-combat-effectiveness-after-ukraine.
77 Macak, K. (2025), 'Cyber warfare and its limits: A response to Soesanto and Gajos', Lawfare, 24 November 2025, https://www.lawfaremedia.org/article/cyber-warfare-and-its-limits--a-response-to-soesanto-and-gajos.
78 ICRC and Geneva Academy Report (2025), 'IHL and the Growing involvement of Civilians in Cyber Operations and other Digital Activities During Armed Conflict', 30 October 2025, https://www.icrc.org/en/publication/ihl-and-growing-involvement-civilians-cyber-operations-and-other-digital-activities.
79 Rodenhäuser, T. and Vignati, M. (2023), '8 rules of "civilian hackers" during war, and 4 obligations for states to restrain them', Humanitarian Law and Policy, 4 October 2023, https://blogs.icrc.org/law-and-policy/2023/10/04/8-rules-civilian-hackers-war-4-obligations-states-restrain-them.

There are some signs that certain cyber proxies are paying attention to the ICRC's rules in the Russia–Ukraine context. In 2023, Killnet told the BBC that it agreed to the ICRC's rules, as did the IT Army of Ukraine, a hacktivist group acting in support of Ukraine.[80] Killnet's leader translated the principles into Russian and circulated them on Telegram. The conversation is certainly a step in the right direction, but other hacktivist groups have not agreed to follow the rules.[81] Given the unprecedented and growing numbers of non-state actors involved in armed conflict, and the ease with which they can participate through digital means, there is a need for more outreach to – and education of – states, individuals, hacker groups and companies on the relevant risks and obligations.[82]

International criminal law

Cyber proxy activity could amount not only to a violation of IHL but also to a war crime. In December 2025, the Office of the Prosecutor of the International Criminal Court (ICC) published a policy on 'Cyber-Enabled Crimes under the Rome Statute'. The policy indicates the Prosecutor's intention to treat international crimes perpetrated or facilitated by cyber means in the same way as more traditional crimes, where cyber activity forms part of the conduct or substantially contributes to the commission of the crime.[83] Under the Rome Statute, international crimes include genocide, crimes against humanity, war crimes and the crime of aggression. Since international criminal law applies to individuals, not states, international criminal responsibility does not depend on attribution of a proxy's activity to a state. Cases may be brought before the ICC through a referral by a state party, by the UN Security Council, or on the Prosecutor's own initiative.

States can also bring domestic prosecutions under international criminal law. Indeed, in the first instance, it is for states to investigate and prosecute international crimes. But in order to do so, they need to have domestic law in place that criminalizes the conduct concerned and gives them jurisdiction over the crimes.[84]

Responsibility under international criminal law can arise not just through perpetration of an international crime but also through other modes of liability, including assistance in the commission of a crime. Where the actions of a cyber proxy make a substantial contribution to the crime, and are conducted for the purpose of facilitating the commission of a crime (for example, if a non-state actor provided online surveillance for the purpose of guiding lethal strikes by Russia that intentionally targeted civilians in Ukraine), the individual may

---

80 Tidy, J. (2023), 'Ukraine cyber-conflict: Hacktivist gangs vow to de-escalate', BBC News, 6 October 2023, https://www.bbc.co.uk/news/technology-67029296.
81 Ibid.
82 See ICRC (2025), 'IHL and the Growing Involvement of Civilians in Cyber Operations and Other Digital Activities During Armed Conflict', 30 October 2025, https://www.icrc.org/en/publication/ihl-and-growing-involvement-civilians-cyber-operations-and-other-digital-activities.
83 International Criminal Court (2025), Office of the Prosecutor, 'Policy on Cyber-Enabled Crimes under the Rome Statute', 3 December 2025, https://www.icc-cpi.int/news/policy-cyber-enabled-crimes-under-rome-statute. For analysis of this policy, see Wilmshurst, E., Moynihan, H. and van Benthem, T. (2026), *Securing justice for cyber-enabled international crimes: Legal foundations and practical routes to prosecution*, Research Paper, London: Royal Institute of International Affairs, https://www.chathamhouse.org/2026/01/securing-justice-cyber-enabled-international-crimes.
84 For discussion of this, see Wilmshurst, Moynihan and Van Benthem (2026), *Securing justice for cyber-enabled international crimes*, pp. 31–34.

be responsible under international criminal law.[85] Not only civilian hackers but also commercial actors, such as the CEOs of Russian hosting providers that offer essential infrastructure and services for the Russian military to carry out attacks on Ukraine, may incur responsibility under international criminal law if the elements of the crime are satisfied.[86]

The Ukrainian State Security Service (SBU) has stated that it is gathering evidence of cyberattacks on Kyivstar, Ukraine's biggest telecom operator; that it has attributed these attacks to Sandworm (a hacker group integrated with Russia's GRU); and that it is submitting the evidence to the ICC for prosecution as war crimes.[87] In June 2024, it was reported that the ICC's investigation in Ukraine covers activity that includes cyberattacks on critical infrastructure.[88] The ICC is also supporting the Joint Investigation Team, made up of six European countries and Ukraine, that is looking into alleged international crimes committed in Ukraine.[89]

Rules on state responsibility

Secondary rules of state responsibility set out the circumstances in which states are liable for cyber activity attributable to them that violates international obligations.[90] These rules also inform the options that victim states can take in response. As noted in Chapter 2, victims of harmful cyber activities by Russia's proxies include not only Ukraine but also Ukraine's allies in the West.[91]

Attribution of a malicious cyber operation involves different elements: technical, political and legal. Attribution is a crucial first step that informs many of the response options for states, in relation to proxies, that will be discussed later in this paper. These options include diplomatic measures, sanctions, countermeasures and prosecutions.

Technical attribution

Technical attribution identifies the source of cyber activity through forensic analysis of malware, network infrastructure and operational patterns. This work is conducted by a range of entities, including government agencies, private cybersecurity firms with specialized capabilities, and sometimes civil society organizations such as Bellingcat or the CyberPeace Institute. Attribution of cyber operations to specific actors is challenging due to the cross-border nature of such operations and the deliberate and sophisticated use of obfuscation, intermediaries

85 For a detailed discussion, see Ibid.
86 Ibid.
87 Antoniuk, D. (2024), 'Ukraine gathers evidence to prosecute hackers behind Kyivstar attack in Hague', The Record, 4 April 2024, https://therecord.media/kyivstar-cyberattack-war-crimes-prosecution-ukraine.
88 Deutsch, A., van den Berg, S. and Pearson, J. (2024), 'Exclusive: ICC probes cyberattacks in Ukraine as possible war crimes, sources say', Reuters, 14 June 2024, https://www.reuters.com/world/europe/icc-probes-cyberattacks-ukraine-possible-war-crimes-sources-2024-06-14.
89 Eurojust (undated), 'Joint investigation team into alleged crimes committed in Ukraine', https://www.eurojust.europa.eu/joint-investigation-team-alleged-crimes-committed-ukraine. The countries involved are Ukraine, Estonia, Latvia, Lithuania, Poland, Romania and Slovakia.
90 The Rules on State Responsibility are set out in the International Law Commission's Articles on State Responsibility, many of which reflect customary international law: UN (2001), 'Responsibility of States for Internationally Wrongful Acts', https://legal.un.org/ilc/texts/instruments/english/draft_articles/9_6_2001.pdf.
91 See, for example, the December 2025 wiper attack against Poland's energy grid, attributed by a private company to Sandworm. Antoniuk, D. (2026), 'Cyberattack on Poland's power grid hit around 30 facilities, new report says', The Record, 28 January 2026, https://therecord.media/poland-electrical-grid-cyberattack-30-facilities-affected.

and false flags. Technical evidence sufficient for operational disruption often cannot be disclosed publicly without compromising intelligence sources. Nevertheless, public–private partnerships and shared threat intelligence have significantly enhanced attribution capabilities, enabling more frequent political attributions (see below).[92]

Political attribution

Political attribution involves a state publicly 'naming and shaming' another state or state-sponsored entity for carrying out malicious cyber activity, based on technical findings and intelligence assessments. This typically occurs through a public statement or press release. For example, in 2024 Germany's foreign ministry publicly linked Russia-connected threat actors to multiple incidents, including an APT28 campaign against German air traffic control and a Storm-1516 information operation targeting electoral integrity.[93] In 2025, several European governments issued statements accusing Russia of cyber interference in critical infrastructure and democratic processes.[94]

The calling out of the state and individuals concerned in such instances has the value of revealing that the state making the attribution has evidence of the activity and identity of the perpetrators. Such statements also create diplomatic pressure on the accused state, and reinforce the normative force of the Framework for Responsible State Behaviour in Cyberspace. As discussed further in Chapter 4, public political attributions can be most effective when accompanied by other measures that impose costs on the accused state. These can include lawful but unfriendly measures (known as 'retorsion') such as diplomatic protests and the expulsion of diplomatic personnel,[95] or the imposition of sanctions such as asset freezes on the individuals concerned.

Legal attribution

For a state to be held responsible under international law, the act concerned must both be attributable to a state under the rules on state responsibility and constitute a violation of international law. In 2018, the then UK attorney general, Jeremy Wright, made the following statement in a speech about the application of international law to cyberspace:

> And international law is clear – states cannot escape accountability under the law simply by the involvement of such proxy actors acting under their direction and control.[96]

---

92 Brock, J. and Lewis, J. (2025), 'Mutual Defense in Cyberspace: Joint Action on Attribution', CSIS, 17 September 2025, https://www.csis.org/analysis/mutual-defense-cyberspace-joint-action-attribution.
93 CERT-EU (2025), 'Cyber Brief (December 2025)', 5 January 2025, Version: 1, https://cow-prod-www-v3.azurewebsites.net/publications/threat-intelligence/cb26-01/pdf.
94 Council of the EU (2025), 'Hybrid threats / Russia: Statement by the High Representative on behalf of the EU condemning Russia's persistent hybrid campaigns against the EU, its Member States and partners', 18 July 2025, https://www.consilium.europa.eu/en/press/press-releases/2025/07/18/hybrid-threats-russia-statement-by-the-high-representative-on-behalf-of-the-eu-condemning-russia-s-persistent-hybrid-campaigns-against-the-eu-its-member-states-and-partners; and Badohal, K. (2025), 'Poland says Russia is trying to interfere in presidential election', Reuters, 6 May 2025, https://www.reuters.com/world/europe/poland-says-russia-is-trying-interfere-presidential-election-2025-05-06.
95 As Albania did in 2022 in response to cyber operations against it that Albania attributed to Iran; see Gritten, D. (2022), 'Albania severs diplomatic ties with Iran over cyber-attack', BBC News, 7 September 2022, https://www.bbc.co.uk/news/world-europe-62821757.
96 Attorney General's Office (2018), 'Cyber and International Law in the 21st Century', speech of Jeremy Wright QC MP, 23 May 2018, https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century.

However, in practice it is difficult for a state to be held legally responsible for an activity of a proxy – both due to the high thresholds of attribution in international law and states' reluctance to invoke international law in relation to cyber activity. The following section analyses the rules on attribution and illustrates why in practice the behaviour of proxy actors will often not be able to satisfy these rules.

Thresholds of attribution under the law on state responsibility

The main bases for legal attribution in international law are Articles 4, 5, 8 and 11 of the Articles on State Responsibility. The applicability of each of these articles to cyber proxies is considered below:

State organs

Under Article 4 of the Articles on State Responsibility, **the conduct of a state organ is attributable to a state**. The test to determine attribution is whether the entity concerned is incorporated into the state's apparatus as a matter of law. Article 4 would cover cyber defence groups such as the Estonian Defence League's Cyber Unit; hacker groups incorporated into a state's apparatus, such as Unit 61398 of the Third Department of the Chinese People's Liberation Army; Israel's Unit 8200; or Bureau 121, a hacking unit with the North Korean Reconnaissance General Bureau.[97] The unit must be completely dependent on the state and have no real autonomy in decision-making. Cyber groups or companies that are contracted by the state to carry out cyber operations may be included, but this depends on the terms of contract and may be hard to prove.[98]

The activities of the GRU are attributable to Russia because, as a military intelligence agency of the General Staff of the Russian Armed Forces, the GRU is an organ of the state.[99] APT units within the GRU are also likely to be considered as state organs under Article 4. The US indictment of *Andrienko and Others* (2020), in which six GRU operatives were accused of deploying destructive malware worldwide (including in the NotPetya operation), states that 'Sandworm' is part of the GRU and therefore the Russian state:

> [T]he GRU … was comprised of multiple units, including Military Unit 74455, which was known within the GRU as the 'Main Center for Special Technologies' … and by cybersecurity researchers as Sandworm Team, Telebots, Voodoo Bear and Iron Viking.[100]

Persons or entities 'empowered to exercise governmental authority'

Under Article 5 of the Articles on State Responsibility, **conduct can be attributed to a state where the person or entity is not an organ of the state but has been empowered by national law to exercise elements of governmental authority**. This might cover, for example, private companies performing public

---

97 See Tsagourias, N. and Farrell, M. (2020), 'Cyber Attribution: Technical and Legal approaches and Challenges', *EJIL* Vol 31(3), p. 951.
98 Ibid.
99 See, for example, the US Department of Justice's indictment of several individuals working for the GRU involved in the WhisperGate campaign against Ukraine in advance of the full-scale invasion in February 2022 in *US v. Stigal*, https://www.justice.gov/archives/opa/pr/five-russian-gru-officers-and-one-civilian-charged-conspiring-hack-ukras inian-government.
100 U.S. District Court Western District of Pennsylvania, *U.S. v. Andrienko and Others*, Indictment filed on 15 October 2020, https://www.justice.gov/archives/opa/press-release/file/1328521/dl.

functions such as providing security. The conduct of cyber proxies contributing to Russia's war effort against Ukraine could only satisfy this test if the proxy were empowered, under Russian domestic law, to provide assistance to Russia; this is a high bar and is likely to be difficult to prove.[101] In particular, there are challenges in distinguishing private from official conduct, although this may be easier to prove where the conduct in question is systematic and recurrent, such that the state ought to have known about it. For example, it has been argued that the systematic and widespread activities of Russian agencies that sought to influence the 2016 US presidential election may be attributed to Russia under Article 5, even if some of the conduct was private in nature.[102]

Acting under the direction, control or instructions of a state

Under Article 8 of the Articles on State Responsibility, **the conduct of a person or group of persons acting on the instructions of, or under the direction and control of, a state is attributable to that state**. Effectively, this is the state using a proxy as its auxiliary to carry out a task – for example, contracting a cybersecurity company to install malware on a computer.[103] In Table 1, above, on the classification of cyber proxies, entities in the category listed as 'APT-commissioned proxies' may in some cases meet the test in Article 8, depending on the level of control exerted over them by the relevant APT.

From international case law, two tests have emerged for determining the degree of control that must be exercised by a state in order for the conduct of a non-state actor to be attributable to that state. The International Court of Justice (ICJ) has held that the test amounts to 'effective control' rather than a general situation of dependence and support.[104] Merely suggesting operational targets, or providing financial support, will not in itself be enough to meet the threshold in Article 8. Similarly, a state simply tolerating the activity of a proxy, turning a blind eye to such activity, or gently encouraging the activity from a distance will not be responsible for the activity in question. However, as noted earlier, the International Criminal Tribunal for the former Yugoslavia (ICTY) found a test of 'overall control' when discussing state control over organized state groups in the context of an armed conflict.

Major Russia-based cybercrime groups that operate 'ransomware as a service' – such as LockBit (featured in the second row of Table 1 above) – would be unlikely to meet the high thresholds of Article 8, but attribution will depend on the facts in each case. In any event, attribution assessments need to be kept under constant review because, as noted earlier, relations between proxies and the state are dynamic. For example, while the Wagner Group is a private military company conducting operations (including information operations) with Russian state backing, it was not part formally of the Russian military. However, since the

---

101 See Tsagourias and Farrell (2020), 'Cyber Attribution', p. 952, which notes that it is highly unlikely that a state will explicitly authorize an entity to perform such activities.
102 Ibid., p. 952.
103 Schmitt and Vihul (2014), 'Proxy Wars in Cyber Space', p. 62.
104 See ICJ (1986), 'Military and Paramilitary Activities in and Against Nicaragua (*Nicaragua v. US*), Merits, Judgment', Rep. 14, paras 109 and 115; and Crawford, J. (2002), *The International Law Commission's Draft Articles on State Responsibility: Introduction, Text and Commentaries*, Cambridge University Press, Commentary to Article 8, para 4.

death of the company's leader, Yevgeny Prigozhin, in 2023, the Russian Ministry of Defence now directly oversees many of the African operations previously run by Wagner, thus bringing them under greater state control.[105]

Acknowledgment and adoption

Finally, Article 11 of the Articles on State Responsibility covers **conduct that is not attributable to a state under other articles, but which can nevertheless be considered an act of a state if that state acknowledges and adopts the conduct as its own**. Acknowledgment and adoption should be distinguished from mere support or endorsement.[106] Sometimes a state acknowledges after the event that non-state actors have played a patriotic role in supporting the state. Under this article, if the state in question is effectively adopting the conduct as its own or fostering its continuance, this could make the state responsible for that conduct.

In the cyber context, Russia's president, Vladimir Putin, acknowledged the role of patriotic hackers in 2017 when discussing the 'theoretical possibility' that they may have been involved in interference with US elections.[107] Such comments would be unlikely to meet the conditions in Article 11 on their own, but if Putin had gone further and unequivocally endorsed the acts of the hackers as part of a Russian state effort, then this might have done so.

Non-state actors can easily acquire cyber capabilities off the shelf, cheaply and without any dependence on a state – this applies, for example, to ransomware-as-a-service tools.

It has been argued that the high attribution thresholds in the Articles on State Responsibility are ill suited to the realities of modern cyber operations. Some voices have called for different attribution determinants, involving a lower threshold of overall control or 'soft control'.[108] The current attribution criteria were developed in a period in which states used proxies to fight in wars with conventional weapons, such as guns and tanks; these were weapons that in the main only states could provide to proxies. But non-state actors can easily acquire cyber capabilities off the shelf, cheaply and without any dependence on a state – this applies, for example, to ransomware-as-a-service tools. However, changes to the present rules would likely take years to agree, even assuming there was the political will to do so – which would not be the case for those states that seek to benefit from the challenges of attribution. A more fruitful approach may be to focus on holding states responsible for harbouring and inciting malicious cyber actors on their territory, as discussed later in this chapter.

---

105 ACLED (2025), 'The Wagner Group and Africa Corps', https://acleddata.com/armed-group/wagner-group-and-africa-corps.
106 See Crawford (2022), *The International Law Commission's Draft Articles on State Responsibility,* Commentary to Article 11, para 6.
107 Harding, L. and Luhn, A. (2019), 'Putin says Russian role in election hacking 'theoretically possible'', *Guardian*, 1 June 2017, https://www.theguardian.com/world/2017/jun/01/putin-says-russian-role-in-election-hacking-theoretically-possible.
108 Tsagourias and Farrell (2020), 'Cyber Attribution', p. 943.

Even if proxy activity can be attributed to a state under the Articles on State Responsibility, it will also be necessary to establish that a violation of international law has occurred in order for that state to be legally responsible. In principle, the activities of a cyber proxy that are attributable to states – whether the proxy actor is conducting cyber operations against the critical infrastructure of a state or information operations in that state – may engage a number of rules of international law, including sovereignty, the prohibition on intervention in another state's internal or external affairs, or international human rights law. For example, in their national positions on the application of international law in the cyber context, several states argue that a cyber operation against a state's critical infrastructure, such as to interfere in a state's electoral infrastructure to manipulate the vote, could violate the prohibition on intervention.[109] A large-scale cyber campaign of disinformation, intended to sow distrust or sway public opinion (for example, encouraging citizens not to take a vaccine during a pandemic), could also violate the prohibition on intervention in certain circumstances[110] as well as engaging obligations under international human rights law.[111] The assessment of legality has to be conducted on a case-by-case basis with reference to the facts.

However, while there have been many public political attributions to date, no state has explicitly connected these to a violation of international law. Indeed, states rarely refer to international law at all when making political attributions, although sometimes they refer to international norms and rules in general terms.[112] There are several reasons for this.[113] Firstly, there is the unsettled state of the law in this area: states continue to discuss how international law applies in cyberspace and have differing views on the application of some rules, such as on sovereignty. Second, states may not wish to invoke a violation of international law for political reasons (e.g. for fear of retribution by the accused state). Some states prefer ambiguity around the rules, to give them flexibility to engage in cyber operations of their own. Even if states do wish to invoke international law (an option likely to be more attractive to less powerful states), they may lack evidence to back up the claim with sufficient confidence.[114]

Response options where legal attribution is established

While states rarely refer to international law in public when making political attribution, they do carry out legal assessments internally. If it can be established that another state is responsible for proxy cyber activity that violates international law, several options are available to the state that is the victim of the malicious

---

109 See, for example, the national positions of Australia, Austria, Brazil, Canada, Germany, Israel, New Zealand, Norway, Singapore, the UK and the US in the Cyber Law Toolkit: 'Scenario 01: Election interference', https://cyberlaw.ccdcoe.org/wiki/Scenario_01:_Election_interference#Prohibition_of_intervention.
110 See van Benthem, T., Dias, T. and Hollis, D. (2023), 'Information Operations under International Law', *Vanderbilt Journal of Transnational Law*, Vol. 55, Iss. 5, 1217, https://scholarship.law.vanderbilt.edu/vjtl/vol55/iss5/4/, p. 1255–1261.
111 For a discussion of how positive and negative obligations of international human rights law apply to information operations, see Ibid., pp. 1232–1254.
112 For example, when the UK attributed cyber operations against UK organizations developing vaccines to Russia, the British foreign secretary condemned the operations as 'unacceptable' and noted that international law and the norms of responsible state behaviour must be respected.
113 For a detailed discussion, see Tsagourias, N. (2024), 'Cyber disputes as legal disputes', in Tsagourias, N., Buchan, R. and Franchini, D. (eds) (2024), *The Peaceful Settlement of Inter-State Cyber Disputes*, Hart, pp. 36–37.
114 Hollis, D. and Finnemore, M. (2020), 'Beyond Naming and Shaming: Accusations and International Law in Cybersecurity', *EJIL* Vol 31(3), p. 999.

cyber activity. These include the rights to take countermeasures, refer the matter to the UN Security Council or bring an inter-state claim before an international court. Each is considered below.

Countermeasures

Countermeasures can be understood as a unilateral response, by the victim state against the wrongdoing state, that would normally be considered a violation of international law but for the fact that the measures are taken in response to a prior violation of international law by the wrongdoing state. In taking the countermeasure, the victim state seeks to compel the wrongdoing state to (1) stop its unlawful behaviour (if the behaviour is continuing), (2) restore the status quo and (3) provide reparation to the victim state. Due to the risk of abuse, the use of countermeasures is governed by strict conditions, set out in the Articles on State Responsibility.[115]

The countermeasure taken by the injured state must be proportionate to the injury suffered, but need not take the same form as the original violation. For example, a response could consist of the victim state freezing the assets of the wrongdoing state. But sometimes responding in kind may be most effective – examples might include deploying a targeted 'hackback' that disables servers or disrupts cyber infrastructure in the wrongdoing state in order to terminate the wrongful cyber conduct. In practice, it can be hard to know how far states are responding to Russian proxies with countermeasures. Typically states do not frame their responses explicitly as countermeasures, and the measures in question, if cyber-related, are often taken covertly.

Several states have confirmed the applicability of the law of countermeasures to cyber operations, including the US, the UK, Australia, Canada, New Zealand, Japan, Singapore and several European states.[116] Other states, including Brazil, China and Cuba, view countermeasures with more caution.[117]

It should be noted that countermeasures are peacetime measures. In the context of the current Russia–Ukraine war, they are therefore relevant as a potential response by Ukraine's allies rather than as an option for Ukraine.[118] Countermeasures cannot involve the use of force. The only situation in which force could be used in response to proxy activity would be if a proxy's cyber activity reached the level of an 'armed attack'.[119] In this situation, some argue that the right of self-defence under the UN Charter would permit the use of force that is both necessary and proportionate

---

115 Article 42 of the Articles on State Responsibility. For a discussion of the relevant requirements and conditions governing countermeasures, and their application in the cyber context, see Dias, T. (2024), *Countermeasures in international law and their role in cyberspace*, Research Paper, London: Royal Institute of International Affairs, https://www.chathamhouse.org/2024/05/countermeasures-international-law-and-their-role-cyberspace.
116 See Cyber Law Toolkit: 'Countermeasures', https://cyberlaw.ccdcoe.org/wiki/Countermeasures.
117 Ibid. A few states consider that countermeasures can be exercised collectively in response to a violation of international law that affects the whole international community or a group of states that have a common interest, or even that countermeasures can be exercised by one state on behalf of another, but these positions are not established as a matter of customary international law. See Buchan, R. (2024), 'Collective and Third Party Cyber Countermeasures', in Tsagourias, Buchan and Franchini (eds) (2024), *The Peaceful Settlement of Inter-State Cyber Disputes*.
118 Ukraine's response options will primarily be governed by IHL since the country is in an armed conflict with Russia.
119 States generally agree that cyber operations that cause significant physical damage, destruction, death and injury can qualify as armed attacks; there is debate over whether a lesser degree of damage or harm may qualify. See Cyber Law Toolkit: 'Use of force', https://cyberlaw.ccdcoe.org/wiki/Use_of_force.

against a proxy when the state in which that proxy is located is unable or unwilling to take action to stop the proxy's activities.[120] Other commentators maintain that the use of force would only be permissible if the proxy's activity is attributable to a state.[121]

In exceptional situations, where there is a grave and imminent peril to an essential interest of the state, and the action is the sole means of safeguarding that interest, a state may be able to act to safeguard its interest, including against non-state actors, and justify its action under the plea of necessity.[122] Unlike with countermeasures, there would be no need to attribute the malicious cyber conduct to a state, which in the proxy context would be beneficial to the victim state. Several European states, the EU and Japan have endorsed application of the plea of necessity in the cyber context.[123] However, the plea of necessity is governed by stringent conditions, including that the response must not seriously impair the essential interests of any other state, and must be direct, proportionate and necessary.[124]

Referral to the UN Security Council

Cyber proxy activity that amounts to a threat to the peace, a breach of the peace or an act of aggression could trigger the UN Security Council's enforcement powers under Chapter VII of the UN Charter. This could include the council adopting a resolution that condemns states for threatening peace and security through malicious cyber operations. The council can also condemn states for allowing non-state actors to operate from their territory, if there is strong evidence of such activity,[125] and can condemn the non-state actors involved as well.

The UN Security Council has not yet adopted a resolution specifically in relation to malicious cyber operations, although these have been mentioned in the council's debates. For example, Estonia raised Russian attacks against Georgia in the UN Security Council in March 2020. Estonian Foreign Minister Urmas Reinsalu stated: 'The intention of the cyber operation organized by the Russian Military Intelligence Service, the GRU, was to discredit Georgia and create confusion. This is yet another example of irresponsible behaviour and violation of stability in cyberspace by Russia.' He added, 'Raising this issue today at the UN Security Council table is historic, and demonstrates that behaviour undermining the cyberspace stability is not being ignored.'[126] A draft resolution proposed by the US in 2022 for strengthening sanctions against North Korea provided a detailed description of malicious cyber activities by the Lazarus Group, a North Korean state-sponsored hacker group, with attribution made by a UN Panel of Experts based on information submitted by member states and through its own

---

120 Article 51 of the UN Charter; see Schmitt, M. and Johnson, D. (2021), 'Responding to Proxy Cyber Operations Under International Law', 6(4) *Cyber Defense Review* 15–30, p. 28, noting that the majority of the International Group of Experts in the *Tallinn Manual 2.0 on International Law Applicable to Cyber Operations* supported this position, as do the US and Israel.
121 For example, the 'Common Position of the African Union on the Application of International Law to the Use of Information and Communication Technologies in Cyberspace', issued on 29 January 2024 by the African Union Peace and Security Council, para 43; see also *Legal Consequences of the Construction of a Wall in the OPTs*, para 139; *Armed Activities in the Congo*, para 168.
122 See Article 25 of the International Law Commission's Articles on State Responsibility.
123 See Cyber Law Toolkit: 'Plea of necessity', https://cyberlaw.ccdcoe.org/wiki/Plea_of_necessity.
124 Chatham House (2023), 'Applying the Plea of Necessity to Cyber Operations', Meeting Summary, 27 September 2023, https://chathamhouse.soutron.net/Portal/Public/en-GB/RecordView/Index/204643.
125 Mikanagi, T. (2024), in Tsagourias, Buchan and Franchini (eds) (2024), *The Peaceful Settlement of Inter-State Cyber Disputes*, p. 141.
126 ERR News (2020), 'Estonia raises cybersecurity issues at UN for first time', 6 March 2020, https://news.err.ee/1060642/estonia-raises-cybersecurity-issues-at-un-for-first-time.

research. The draft resolution attracted strong support but was vetoed by China and Russia.[127] As this example reflects, use of the veto power significantly limits this route to accountability in practice.

An inter-state claim

A state that is the victim of a malicious cyber operation carried out by a proxy actor could have recourse to dispute settlement mechanisms, for example by bringing an inter-state case before an international court such as the ICJ. The ICJ currently has an unprecedented 24 contentious cases on its docket, and an increasing number of states are intervening in cases.[128] Ukraine has brought several inter-state claims before international tribunals in relation to Russia's aggression against it, including some claims that have involved the attribution of proxies' conduct to Russia. For example, in *Ukraine and The Netherlands v. Russia*, the European Court of Human Rights held that armed separatists in eastern Ukraine were under Russia's control ('once the armed separatists were formerly integrated into the military hierarchy of the Russian armed forces, they had the legal status of State organs, and were, accordingly, from that date *de jure* organs of the respondent State within the meaning of Article 4 ARSIWA').[129]

Ukraine has brought several inter-state claims before international tribunals in relation to Russia's aggression against it, including some that involved the attribution of proxies' conduct to Russia.

However, there are several challenges to inter-state litigation, particularly in the cyber context. First, it will be necessary to establish the existence of a dispute between two states. As noted above, to date states have refrained from characterizing cyber activity as a violation of international law or from framing the issue as a 'cyber dispute'.[130] States accused of malicious cyber activity are also unlikely to consent to an international court's jurisdiction over the case.[131] Even if they do so, evidence is likely to be difficult to obtain, as proxies employ tactics to hide their identity and location. States may also not wish to disclose evidence in court if this evidence has been obtained through intelligence or through the searching without consent of other states' computer networks.[132]

---

127 Ibid., pp. 139–141.
128 Wentker, A. (2024), 'More and more cases on war and genocide are being litigated at the ICJ', Chatham House Expert Comment, 4 September 2024, https://www.chathamhouse.org/2024/09/more-and-more-cases-war-and-genocide-are-being-litigated-icj.
129 ECtHR, *Ukraine and The Netherlands v. Russia,* Applications nos. 8019/16, 28525/20 and 11055/22, 9 July 2025, para 364.
130 Antonopoulos, C. (2024), 'Cyber Disputes before the ICJ: Issues of Jurisdiction and Admissibility' in Tsagourias, Buchan and Franchini (eds) (2024), *The Peaceful Settlement of Inter-State Cyber Disputes*.
131 But see Moynihan, H., Webb, P. and Clooney, A. (2025), 'Legal Accountability for Malicious Cyber Operations', Policy Brief, Oxford Institute of Technology and Justice, September 2025, noting that compromissory clauses may provide a potential basis of claim on certain fact patterns, pp. 26–27 and 31–33.
132 The legal position on such extraterritorial activity is currently unsettled; see national position of the Netherlands in the Cyber Law Toolkit: https://cyberlaw.ccdcoe.org/wiki/Sovereignty#Netherlands_(2019).

There have been no international cyber disputes to date, but it is likely that states will seek to test this route in the future.[133] We can also expect to see cases in which a cyber element features as part of a wider claim.

Response options where legal attribution cannot be established

Where the conduct of a proxy cannot be attributed to a state, but the identity of the proxy can be identified through technical attribution, there are other measures that can be invoked in response to the harmful behaviour. Political and diplomatic responses, including acts of retorsion, have already been discussed above. The principle of due diligence is also important in this context.

Due diligence

In 2015, the UN Group of Government Experts (GGE) agreed 11 norms of responsible behaviour in cyberspace ('the UN cyber norms'), one of which was that 'States should not knowingly allow their territory to be used for internationally wrongful acts using ICTs'.[134] The 2015 GGE report applied this norm specifically to proxies, affirming that 'States must not use proxies to commit internationally wrongful acts using ICTs, and should seek to ensure that their territory is not used by non-State actors to commit such acts'.[135] The principle of due diligence is reflected in various sources of international law, including the case law of the ICJ, certain rules of IHL (as noted above), obligations under international human rights law, and the no-harm principle in environmental law.[136]

The exact measures to be taken by the state on whose territory malicious cyber actors are operating will depend on the state's capacity and the facts in each case, since due diligence is an obligation of conduct rather than result.[137] Domestic measures might include taking steps to monitor cyber activity in the territory in question; ensuring the ability to communicate swiftly with international partners to provide notification of the malicious cyber activity by establishing robust computer emergency response teams (CERTs); and criminalizing harmful cyber activity.

At the international level, states have strengthened cooperation and notification systems (including through the UN's Point of Contact Directory), such as enhancing CERT-to-CERT cooperation. Under the Framework for Responsible State Behaviour in Cyberspace, this is a practical example of a **confidence-building** measure that can strengthen trust between states in tackling malicious cyber activity and reduce the risk of escalation. But **capacity-building** is also important, since the investigation and prosecution of cyber operations is costly and resource-intensive.

---

133 See Moynihan, Webb and Clooney (2025), 'Legal Accountability for Malicious Cyber Operations'.
134 Norm (c) of the UN cyber norms: Australian Strategic Policy Institute (2022), 'The UN norms of responsible state behaviour in cyberspace: Guidance on implementation for Member States of ASEAN', March 2022, https://www.aspi.org.au/report/un-norms-responsible-state-behaviour-cyberspace.
135 UNGA (2015), 'Report of UN GGE', UN Doc A/70/174, 28 July 2015, para 28(e).
136 See Coco, A. and Dias, T. (2021), 'Cyber Due Diligence: A Patchwork of Protective Obligations in International Law', *EJIL*, Vol 32(3).
137 For a discussion of the obligations involved and what they may require, see Ibid.

Capacity-building will be a priority for a new body, the UN Global Mechanism, which started work in March 2026 as a permanent forum for ongoing discussion of information security issues. However, the same challenges that hindered consensus in the Open Ended Working Group (OEWG) on Security of and in the Use of Information and Communications Technologies (ICTs) remain; indeed, the challenges are arguably heightened by today's tense geopolitical climate and the relative absence of a US leadership role comparable to Russia's influence at these meetings. Consequently, expectations for progress on accountability for proxy activities and for states to fully abide by the norms are limited.[138]

Legal status

While the UN cyber norms are not legally binding on states, some states and scholars argue that norm (c), which derives from the ICJ's *Corfu Channel* case,[139] reflects a binding obligation. Indeed, the majority of states that have published national positions on the application of international law to cyberspace so far assert that due diligence is a binding obligation that applies in the cyber context; the same is true of the EU and African Union in their common positions.[140]

As noted above, a violation of international law gives the injured state the right to take countermeasures under certain circumstances, and some states, such as France and Switzerland, have explicitly mentioned the right to take countermeasures where the due diligence obligation is violated.[141] This is pertinent in the Russia–Ukraine context since the Russian government has not shown any sign of investigating the significant amount of cybercrime originating in Russia,[142] some of which is reported to be part of Russia's hybrid warfare operations.[143] Indeed, Russia turns a blind eye to the activities of the perpetrators and denies that it is responsible for such incidents.[144]

If a countermeasure were permitted in this context, the question would arise as to its permissible scope: whether it must be taken against the host state, or whether it could be taken directly against the proxy actor to supplement the failing state's law enforcement obligation. Some scholars argue that while countermeasures are designed to target the legal interests of the wrongdoing state, there is no requirement that they be directed against the state itself, and that therefore it is possible to target non-state actors.[145]

---

138 Korzak, E. (2025), 'New UN permanent mechanism on cybersecurity is saddled with old controversies', Binding Hook, 4 September 2025, https://bindinghook.com/new-un-permanent-mechanism-on-cybersecurity-is-saddled-with-old-controversies.
139 Corfu Channel (*UK v. Albania*), Judgment (Merits) [1949] ICJ Rep 4.
140 Cyber Law Toolkit: 'Due diligence', https://cyberlaw.ccdcoe.org/wiki/Due_diligence#:~:text=In%20the%20context%20of%20cyberspace,right%20of%20another%20state%3B%20and.
141 Ibid.
142 University of Oxford, Department of Sociology (2024), 'World-first Cybercrime Index maps the global geography of cybercrime', 10 April 2024, https://www.sociology.ox.ac.uk/article/world-first-cybercrime-index-ranks-countries-by-cybercrime-threat-level.
143 See, for example, Dickson, J. and Harding, E. (2025), 'How Cyber Alliance Took Down Russian Cybercrime', Center for Strategic Studies, 28 July 2025, https://www.csis.org/analysis/how-cyber-alliance-took-down-russian-cybercrime.
144 Deutsch, A. and Meijer, B. (2025), 'Russia is ramping up hybrid attacks against Europe, Dutch intelligence says', Reuters, 22 April 2025, https://www.reuters.com/world/europe/russia-is-upping-hybrid-attacks-against-europe-dutch-intelligence-says-2025-04-22.
145 Schimtt, M. (2015), 'In Defense of Due Diligence in Cyberspace', The Yale Law Journal Forum, 22 June 2015, p. 79, https://yalelawjournal.org/pdf/Schmitt_PDF_g9pv96jc.pdf.

However, several states – including the US, the UK, Canada, Israel and New Zealand – consider that the principle of due diligence does not have the status of customary international law.[146] The legal status of the norm is thus unsettled; indeed, the status of due diligence in international law generally remains a question of debate.[147]

Other issues that remain unsettled are the standard of knowledge required to trigger due diligence obligations on the part of a host state (for example, whether it should be actual or constructive knowledge of the harmful cyber activity taking place on the state's territory), and whether due diligence requires preventative measures or simply reasonable measures within that state's capacity to bring the harmful activity to an end.[148] Therefore, while many states agree that due diligence is important as at the very least an expectation of responsible behaviour in the cyber context,[149] Russia's long-standing failure to abide by the due diligence principle means that due diligence is likely to be of limited practical effect in constraining Russia's use of cyber proxies. However, norm (c) and the due diligence principle are useful in encouraging other states to build up their capacity to cooperate on the investigation and prosecution of malicious cyber activity emanating from Russia, as discussed further in Chapter 4 below.

In addition, there would be value in ensuring that the accountability of states for harbouring and inciting malicious cyber activity on their territory is factored into frameworks being developed in other contexts – for example the work of the UN Working Group on the Use of Mercenaries mentioned above, the work of the International Law Commission on due diligence, and discussions about due diligence in the context of the UN Convention against Cybercrime (which focuses primarily on state obligations to prosecute individuals but would benefit from more explicit attention to state responsibility for harbouring or enabling malicious cyber activity).

Lessons should be drawn from accountability models developed in other domains. In particular, the evaluative and listing mechanisms of the Financial Action Task Force (FATF) (which identifies and publicly designates jurisdictions with strategic deficiencies in countering financial crime) and the preventative obligations contained in the United Nations Convention against Transnational Organized Crime (UNTOC) (under which states must actively suppress transnational organized crime rather than merely tolerate its presence) demonstrate that the international system already recognizes expectations of due diligence in tackling serious transnational crime. While the cyber context presents particular challenges – notably with respect to establishing attribution – these frameworks provide useful reference points for approaches to accountability for malicious cyber activity, including the value of an approach based on tackling whole ecosystems rather than particular actors.

---

146 See the sections on due diligence in the national positions of these states, available in Cyber Law Toolkit: 'Due diligence', https://cyberlaw.ccdcoe.org/wiki/Due_diligence.
147 Due diligence in international law is being considered by the UN International Law Commission; see UN International Law Commission (2026), 'Summaries of the Work of the International Law Commission', https://legal.un.org/ilc/summaries/9_13.shtml.
148 Moynihan, H. (2023), 'Unpacking Due Diligence in Cyberspace', *Journal of Cyber Policy*, Vol. 8, 2023.
149 See, for example, the national positions of 28 states plus the common positions of the African Union and European Union, in the Cyber Law Toolkit, 'Due diligence', https://cyberlaw.ccdcoe.org/wiki/Due_diligence.

04 Evaluating disruption and cost imposition measures

Disruption operations, sanctions, prosecutions and diplomatic expulsions have imposed real costs on Russian cyber proxies. But tactical successes have yet to translate into strategic deterrence – this chapter examines why.

Legal frameworks provide important tools for holding states, individuals and private entities accountable for their cyber malicious activity. However, legal measures alone are not sufficient to shape adversaries' behaviour or mitigate ongoing threats. Building on the framework outlined earlier in this paper (see 'Methodology' in Chapter 1), we consider accountability as relying on two mutually reinforcing elements: **disruption**, aimed at degrading proxy capabilities in real time; and **cost imposition**, including the legal but also the financial and reputational measures that increase the price of hostile activity.

Both disruption and cost imposition contribute towards the overarching objective of **deterrence**. Deterrence is achieved not through any single measure, but when disruption and cost imposition are applied credibly, consistently and visibly enough to alter an adversary's decision-making and shape the calculus of that adversary's future operations.

The following sections examine how these two sets of instruments – disruption and cost imposition – have been applied in practice to counter Russian cyber proxies, and the extent to which such efforts have generated meaningful deterrence.

A. Disruption: operational measures targeting proxies

Ukraine and its allies have undertaken a series of disruption operations targeting Russian cyber proxies and state-linked actors, combining technical measures (including domain seizures and server takedowns), law enforcement actions, arrests and civil lawsuits, often in partnership with private sector technology firms. Ukraine's contributions have been particularly significant in real-time threat detection and intelligence sharing through CERT-UA and the SBU.

These measures have achieved tactical success, disrupting specific operations and complicating Russian efforts to conduct hostile activities. However, delays in attribution, proxies' ability to rapidly restore their infrastructure to functionality after damage or disablement, and the incident-driven, reactive nature of the measures involved mean that sustained degradation of proxy capabilities has not been achieved. Even following initially successful disruption efforts, proxies quickly shift to new hosting providers, re-register domains and adopt alternative payment mechanisms. Disruption operations therefore create friction but struggle to dismantle the underlying proxy infrastructure unless they are embedded within a sustained strategy to increase costs and constrain proxy resilience.

Ukraine and its allies have undertaken a series of disruption operations targeting Russian cyber proxies and state-linked actors.

Table 3 highlights major disruption operations that Ukraine and its allies have undertaken, and demonstrates how these operations have targeted proxy infrastructure. The examples illustrate the range of approaches employed – from technical takedowns to legal action to public warnings – and the scale of multinational coordination involved.

Table 3. Major disruption operations against cyber proxies

Type/name of operation	Objectives	Disruption action	Responsible parties
Operation Eastwood (Jun. 2024) – disruption of NoName057(16) hacktivist network.	Dismantle infrastructure; arrest core members; deter recruitment through legal warnings.	Takedown of pro-Russian DDoS hacktivist network including 100+ servers; arrest warrants in Germany and Spain; US indictment of Victoria Eduardovna Dubranova for alleged GRU collaboration (cases not yet concluded);[150] and legal warnings to volunteer supporters.	Europol, Eurojust, 12+ national law enforcement agencies, US Department of Justice (DOJ)
Threat detection and blocking (continuous, 2022–24)	Identify and block malicious infrastructure in real time; prevent compromise of Ukrainian government networks and critical infrastructure.	Real-time detection and blocking of Russian malware and phishing infrastructure; threat intelligence sharing across CERT Ukraine, SBU and Western cybersecurity partners to identify and neutralize malicious campaigns before systems are compromised.	CERT Ukraine, SBU, Western cybersecurity firms
Microsoft-DOJ Star Blizzard/Callisto Group disruption (Oct. 2024)	Disrupt phishing operations; remove espionage infrastructure; impose operational costs on FSB Centre 18 and associated actors.	Seizure of 107 domains used by FSB Centre 18's Callisto Group (tracked by Microsoft as Star Blizzard) and criminal proxies acting on its behalf, for spear-phishing and credential theft targeting government officials, defence contractors, think-tanks, journalists and NGOs.	US DOJ, Microsoft Digital Crimes Unit
Operation Cronos (Feb. 2024) – LockBit takedown	Dismantle ransomware-as-a-service ecosystem; arrest operators; cut financial flows; deter recruitment and further participation by affiliates.	Seizure of LockBit dark-web infrastructure; arrest of affiliates; international arrest warrants and indictments (France, US); cryptocurrency asset freezing.	UK National Crime Agency (NCA), FBI, Europol, Eurojust, US DOJ, 10+ countries

Sources: Compiled by authors.

Technology companies played a key role in these disruption operations, working with law enforcement to disable malicious infrastructure. Microsoft's Digital Crimes Unit, acting concurrently with the US Department of Justice, seized domains used by Russian intelligence proxies (such as Star Blizzard), while cybersecurity firms such as CrowdStrike, Mandiant and Recorded Future provided

150 U.S. Department of Justice (2025), 'Justice Department Announces Actions to Combat Two Russian State-Sponsored Cyber Criminal Hacking Groups'.

threat intelligence and attribution support across a range of similar operations. Nonprofit groups like ShadowServer and abuse.ch aided operations such as Eastwood, mapping infrastructure used by pro-Russian hackers. Commercial intelligence helped dismantle ransomware networks during Operation Cronos. The success of these operations relied on close coordination between government agencies and private sector entities controlling the exploited infrastructure.

B. Cost imposition: legal, financial and reputational measures

In addition to disruption efforts, Ukraine and its allies have increasingly focused on cost imposition measures to ensure cyber operations, especially those by Russian cyber proxies, are met with lasting consequences. These measures are intended not only to deter future attacks but also to raise the costs of recruiting and maintaining proxy actors, making it more difficult for these networks to operate.

This section examines three primary cost imposition tools: cyber sanctions, criminal prosecution and diplomatic retorsion (unfriendly but lawful acts taken in response to the conduct of another state), which together represent the most visible and politically significant accountability mechanisms deployed by states against Russian cyber proxies.

Cyber sanctions

The EU has systematically expanded its cyber sanctions framework in response to Russian proxy operations. Following the June 2024 designation of six individuals for their involvement in malicious cyber operations targeting Ukraine and its allies, the Council of the European Union extended the broader cyber sanctions regime until 2028, signalling sustained political commitment. These sanctions impose asset freezes, travel bans and financial transaction prohibitions on designated actors, though the practical impact of the measures depends heavily on enforcement and the geographic and political reach of sanctioning authorities.[151]

Developed as a component of the EU's 2017 Cyber Diplomacy Toolbox, sanctions form one instrument within a framework designed to provide a graduated spectrum of diplomatic responses to malicious cyber activity – from coordinated statements and démarches (formal diplomatic messages expressing a government's position or request) through to targeted sanctions of the types mentioned above. The toolbox is premised on collective attribution enabling collective response, and in principle represents exactly the kind of integrated,

151 Council of the European Union (2025), 'Cyber-attacks: Council extends sanctions and legal framework', press release, 12 May 2025, https://www.consilium.europa.eu/en/press/press-releases/2025/05/12/cyber-attacks-council-extends-sanctions-and-legal-framework.

strategically coherent framework this paper advocates. In practice, however, it has been underused relative to its ambition, with consensus among member states proving difficult to achieve consistently.[152]

Similarly, the UK imposed sanctions on 18 GRU officers and three military intelligence units in July 2025, explicitly targeting personnel assessed as having been involved in sustained malicious cyber activity against Western institutions and energy infrastructure and in hybrid warfare operations. The designations covered GRU Units 29155 and 26165, both implicated in proxy-linked campaigns, and drew explicit connections between Russian-backed cyber operations and Moscow's broader destabilization efforts.[153] Amplifying the diplomatic signal, NATO and EU allies issued coordinated statements condemning Russian hybrid activities.[154]

The UK has also stepped up sanctions recently in light of escalating hybrid threats, especially in relation to information warfare attributed to Russian proxies; these proxies include Russian think-tanks such as the 'Centre for Geopolitical Expertise' that seek to hide their links to the Russian government.[155]

In November 2025, Canada for the first time sanctioned entities supplying the digital infrastructure used in Russian hybrid strategies against Ukraine; this was alongside designations targeting Russia's drone programme and shadow fleet.[156]

The strategic logic of cyber sanctions rests on several assumptions: that individual actors can be deterred by personal costs, that sanctions signal resolve to domestic and allied audiences, and that cumulative designations raise the operational cost of proxy recruitment and retention. However, the effectiveness of such measures remains difficult to measure. Individuals subject to economic sanctions may have assets seized and be unable to engage in financial transactions touching the US or other sanctioning countries – these risks will be felt at the personal level, and may exert a form of 'micro-level' deterrence.[157] On the other hand, sanctioned individuals often have limited assets in Western jurisdictions, and Russia has demonstrated willingness to absorb reputational costs.

The primary value of current sanctions may therefore lie in normative signalling and coordination rather than immediate behavioural change – communicating that proxy misuse will invoke sustained political consequences even when kinetic or

---

152 The effectiveness of the EU cyber sanctions regime remains debated. While the framework demonstrates political unity and contributes to signalling and norm-setting, analysts note that its operational impact has been limited by the small number of designations and the unanimity requirement governing decisions, which can slow or constrain collective action. See, for example, Saiz Erausquin, G. (2025), 'RUSI Cyber Sanctions Taskforce: Countering State-Backed Cyber Threats', RUSI Insights Paper, 28 October 2025, https://www.rusi.org/explore-our-research/publications/insights-papers/rusi-cyber-sanctions-taskforce-countering-state-backed-cyber-threats; and Bendiek, A. and Schulze, M. (2021), 'Attribution: A Major Challenge for EU Cyber Sanctions', SWP Research Paper 2021/RP 11, Stiftung Wissenschaft und Politik, 16 December 2021, https://doi.org/10.18449/2021RP11.
153 Foreign, Commonwealth & Development Office (2025), 'UK Sanctions Russian Spies at the Heart of Putin's Malicious Regime', press release, 18 July 2025, https://www.gov.uk/government/news/uk-sanctions-russian-spies-at-the-heart-of-putins-malicious-regime.
154 Council of the European Union (2025), 'Hybrid threats / Russia: Statement by the High Representative on behalf of the EU condemning Russia's persistent hybrid campaigns against the EU, its Member States and partners'.
155 Foreign, Commonwealth and Development Office (2025), 'New UK action against foreign information warfare', policy paper, 9 December 2025, https://www.gov.uk/government/publications/new-uk-action-against-foreign-information-warfare/new-uk-action-against-foreign-information-warfare.
156 Global Affairs Canada (2025), 'Minister Anand announces additional sanctions against Russia', press release, 12 November 2025, https://www.canada.ca/en/global-affairs/news/2025/11/minister-anand-announces-additional-sanctions-against-russia.html.
157 See Eichensehr, K. (2020), 'The Law and Politics of Cyber Attribution', 67 *UCLA Law Review* 520, p. 554.

legal responses are unavailable. Whether normative signalling alone can contribute meaningfully to deterrence remains an open question, and one that points to the need for sanctions to be embedded within a broader, coherent response strategy rather than deployed in isolation.

Prosecution under domestic criminal law

As is clear from Table 3 above, prosecution of proxy actors can interact with other accountability measures – political, diplomatic, financial and reputational – to impose costs.

Both Ukraine and its allies increasingly target Russia's proxies with court action. Ukraine has brought prosecutions against Russian hackers under its domestic criminal code. For example, in October 2024 a Ukrainian court sentenced in absentia two members of the Russian Federal Security Service (FSB)-backed hacker group 'Armageddon' for having carried out more than 5,000 cyberattacks against Ukrainian institutions and critical infrastructure. The unnamed hackers previously worked as employees of Ukraine's SBU in occupied Crimea before voluntarily joining the FSB following Russia's annexation of Crimea in 2014.[158]

The US has issued a series of indictments since 2014 in relation to malicious cyber actors from Russia, China, Iran and North Korea. In several high-profile cases, the US has used a multi-pronged strategy of issuing a public statement, imposing sanctions, then issuing an indictment against the individuals concerned.[159] The sequencing of measures will depend on the facts in each case: sometimes, indictments are issued before sanctions, as in the case of US accusations against Iran of DDoS attacks on financial institutions.[160]

The US has indicted suspected cyber proxies apparently operating from Russia, based on extraterritorial jurisdiction. For example, in the case of *US v. Stigal,* a Russian national has been charged with intentional conspiracy to hack into and destroy computer systems and data. The indictment states that the accused 'supported the activities of the GRU by setting up online infrastructure for GRU officers to use in cyberattacks, including in the deployment of the WhisperGate malware'.[161] According to the US Department of Justice, in advance of the full-scale Russian invasion of Ukraine, the targets of Stigal and his alleged co-conspirators included Ukrainian government systems and data with no military or defence-related roles. Later targets included computer systems in countries that were providing support to Ukraine, including the US.[162]

---

158 Basmat, D. (2024), 'Ukrainian court sentences hackers who carried out over 5,000 cyberattacks for Russia', Kyiv Independent, 7 December 2024, https://kyivindependent.com/ukrainian-court-sentences-hackers-who-carried-out-more-than-5-000-cyberattacks-for-russia.
159 See Eichensehr (2020), 'The Law and Politics of Cyber Attribution', p. 537.
160 Ibid.
161 U.S. District Court of Maryland (2024), indictment in *US v. Stigal*, para 6, https://www.justice.gov/d9/2024-06/amin_stigal_unsealed_indictment_0.pdf.
162 U.S. Department of Justice (2024), 'Russian National Charged for Conspiring with Russian Military Intelligence to Destroy Ukrainian Government Computer Systems and Data', 26 June 2024, https://www.justice.gov/archives/opa/pr/russian-national-charged-conspiring-russia-military-intelligence-destroy-ukrainian.

In December 2025, the US charged a Ukrainian national, Victoria Eduardovna Dubranova, with conducting alleged cyberattacks on critical infrastructure worldwide as part of two Russian state-sponsored hacking operations.[163] One operation was said to be with the CyberArmyofRussia_Reborn (known as CARR), which was founded and funded by Russia's GRU, according to prosecutors. CARR is said to have caused damage to the control systems of public drinking water systems in several US states, and resulted in huge water spills; CARR is also alleged to have triggered an ammonia leak and spoiled meat at a processing facility. The second operation in which Dubranova is alleged to have been involved was with the group NoName057(16) (see row 4 of Table 2 and row 1 of Table 3 above), which launched more than 1,500 attacks on government agencies, financial institutions, railways and ports in Ukraine and NATO countries including Estonia, Finland, Lithuania, Norway, Poland and Sweden between March 2022 and June 2025.[164]

Even where a case does not go to trial, the launching of an investigation can bring some immediate benefits.

However, there are various challenges to the investigation and prosecution of cyber proxies. Investigations are time-consuming and expensive, therefore only an option for well-resourced states with strong attribution capabilities. To gather the evidence, states are likely to need to cooperate with service providers or cybersecurity companies on technical attribution. But in some cases, local law, or the terms of service of the companies concerned, may prevent companies from handing over relevant data. Mutual legal assistance procedures for gathering evidence for prosecution are typically slow and bureaucratic, and states may not have the relevant law in place or the resources to prosecute. If the alleged perpetrators are located in Russia, Russia will refuse to prosecute or extradite them (in the *Stigal* case above, the accused remains at large).[165] As a result, there have been relatively few successful prosecutions so far.

Despite these challenges, prosecution of malicious cyber activity is on the rise. Even where a case does not go to trial, the launching of a domestic investigation can bring some immediate benefits. Firstly, it puts partners – states, intergovernmental organizations such as Europol and Interpol, and the private sector, which increasingly work together[166] – on notice of the prosecuting state's

---

163 Otto, G. (2025), 'US charges hacker tied to Russian groups that targeted water systems and meat plants', Cyberscoop, 10 December 2025, https://cyberscoop.com/us-charges-russian-backed-hacker-critical-infrastructure-attacks-carr-noname05716; U.S. Department of Justice (2025), 'Justice Department Announces Actions to Combat Two Russian State-Sponsored Cyber Criminal Hacking Groups'.
164 Otto (2025), 'US charges hacker tied to Russian groups that targeted water systems and meat plants'.
165 The Russian constitution prohibits the extradition of a Russian citizen to another state. See University of Minnesota Human Rights Library (undated), 'The Constitution of the Russian Federation', Article 61(1), https://hrlibrary.umn.edu/research/constitution-russia.html.
166 For example, in June 2025 Microsoft and the cybercrime unit of Europol agreed to partner through a new European security programme. Smith, B. (2025), 'Microsoft launches new European Security Program', Microsoft, 4 June 2025, https://blogs.microsoft.com/on-the-issues/2025/06/04/microsoft-launches-new-european-security-program.

need for evidence to secure prosecution and mobilizes networks of cooperation, for example those established under the Budapest Convention on Cybercrime 2001.[167] Secondly, partner states may choose to provide political or diplomatic support in various ways, for example by participating in collective efforts on attribution or the imposition of sanctions on the individuals or entities concerned. Finally, the launching of a domestic investigation sets up the potential for joint investigations. Since attribution and due diligence come with major challenges in relation to proxies, and since Russia is increasingly conceived as operating in effect as a criminal state,[168] there are clear strategic benefits in states joining forces in investigations and prosecutions. As Table 3 makes clear, several recent operations have proved the effectiveness of this approach, including Germany and Spain issuing arrest warrants for seven suspected members of NoName057(16), a pro-Russian hacking group. These arrests were the result of an international operation involving law enforcement and judicial authorities from several countries, including France, Italy, the Netherlands, Sweden and the US.[169]

The recent adoption of several multilateral instruments is likely to strengthen the prospects for successful prosecution of cyber proxies. In addition to the Budapest Convention on Cybercrime – which has 81 states parties, including the US – the Second Additional Protocol to the Budapest Convention on enhanced cooperation and disclosure of electronic evidence (signed but not yet in force) will enable states parties to obtain electronic data (such as subscriber information and traffic data) directly from service providers located in other countries. This will apply regardless of whether there is a mutual legal assistance treaty (MLAT) – the legal channel that enables states to request and share evidence from criminal investigations and prosecutions – in place.[170] Direct requests by EU member states to service providers for certain electronic data will also be possible under the EU's e-Evidence framework, which will establish uniform rules on the preservation and disclosure of electronic evidence from 2026.[171] The UN Convention against Cybercrime, signed in 2025 by 71 states and the EU, could also be useful for the purposes of collecting, obtaining, preserving and sharing evidence of

---

167 Council of Europe Convention on Cybercrime (Budapest Convention, ETS No. 185), adopted 23 November 2001, entered into force 1 July 2004.
168 See, for example, see Kirillova, K. (2024), 'Russia: When the State Becomes a Criminal', Center for European Policy Analysis, 7 May 2024, https://cepa.org/article/russia-when-the-state-becomes-a-criminal; Karolewski, I. (2023), 'Is Russia now a Criminocracy?', LSE Blog, 23 October 2023, https://blogs.lse.ac.uk/europpblog/2023/10/23/is-russia-now-a-criminocracy.
169 Segreti, G. and Escritt, T. (2025), 'Seven arrest warrants issued in global swoop on suspected Russia-linked hackers', Reuters, 16 July 2025, https://www.reuters.com/technology/seven-arrest-warrants-issued-global-swoop-suspected-russia-linked-hackers-2025-07-16.
170 Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence, CETS No. 224, art. 7. Open for signature 12 May 2022; art. 7.
171 Regulation (EU) 2023/1543 on European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings, which will apply from 18 August 2026, and Directive (EU) 2023/1544 laying down harmonized rules on the designation of designated establishments and the appointment of legal representatives for the purpose of gathering electronic evidence in criminal proceedings, which EU member states are due to have transposed into national law by 18 February 2026, although at the time of writing only five states had adopted implementing legislation. See Bird & Bird (2026), 'EU e-Evidence Directive: Transposition Deadline Reached – Implementation Status and Critical Action Points for Service Providers', 18 February 2026, https://www.twobirds.com/en/insights/2026/germany/eevidencerichtlinie-umsetzungsfrist-abgelaufen--implementierungsstatus-und-handlungsbedarf.

cybercrime.[172] Importantly for the purpose of proxy activity, these treaties do not just apply to ordinary cybercrime such as spamming or computer fraud, but also to malicious cyber activity more broadly (the UN Convention against Cybercrime, for example, applies to 'any serious crime').[173]

Prosecutions also send a signal to the public, as well as to perpetrators, that the prosecuting state has intelligence about where the malicious cyber activity is coming from and has sufficient evidence to prosecute. This has been part of the US's rationale for its 'speaking indictments'.[174] And even if the alleged perpetrator is in a state that refuses to prosecute or extradite, their movement will be restricted, as a person travelling to a country that is prepared to extradite risks being arrested and sent to trial. For example, Russians associated with the Phobos ransomware tool were arrested and extradited from South Korea and Italy for prosecution.[175] In the *US v. Dubranova* case mentioned above, the accused was extradited to the US and is standing trial there. Fear of prosecution may also have a deterrent effect.

Diplomatic retorsion and symbolic costs

Since the start of the war, Ukraine's allies have used diplomatic 'retorsion' – which includes measures such as formal protests and expulsions of diplomats – to signal that hostile cyber and hybrid activities carry political costs. Expulsions of Russian diplomatic personnel since 2022 have been driven by concerns over espionage and destabilizing intelligence operations that may have been carried out under diplomatic cover. Many Western governments have explicitly framed the expulsions as responses to Russia's hybrid campaign – which includes cyberattacks, disinformation and sabotage supporting the war effort against Ukraine.

In March 2022, more than 20 Russian diplomats were expelled by countries including Belgium and the Netherlands, with the authorities claiming that Russian intelligence gathering was being disguised as diplomatic activity.[176] Poland expelled dozens of Russian diplomats that same month on national security grounds. Across Europe, hundreds of Russian diplomatic staff were targeted in coordinated waves of expulsions linked to concerns about espionage and interference supporting Russia's war effort.[177]

---

172 UN Convention against Cybercrime: Strengthening International Cooperation for Combating Certain Crimes Committed by Means of Information and Communications Technology Systems and for the Sharing of Evidence in Electronic Form of Serious Crimes ('UN Cybercrime Convention'), UN Doc A/79/460, https://docs.un.org/en/A/79/460.
173 UN Convention against Cybercrime, art. 35.
174 Hinck, G. and Maurer, T. (2019), 'What's the point of charging foreign state-linked hackers?', Lawfare, 24 May 2019, https://www.lawfaremedia.org/article/whats-point-charging-foreign-state-linked-hackers.
175 Europol (2025), 'Key figures behind Phobos and 8Base ransomware arrested in international cybercrime crackdown', 11 February 2025, https://www.europol.europa.eu/media-press/newsroom/news/key-figures-behind-phobos-and-8base-ransomware-arrested-in-international-cybercrime-crackdown.
176 Euronews (2022), 'EU countries expel dozens of Russian envoys amid war in Ukraine', Euronews, 29 March 2022, https://www.euronews.com/2022/03/29/eu-countries-expel-dozens-of-russian-envoys-amid-war-in-ukraine.
177 Kiyagan, A. (2022), '150 Russian diplomats expelled in Europe since Ukraine war started', Anadolu Agency, 31 March 2022, https://www.aa.com.tr/en/europe/150-russian-diplomats-expelled-in-europe-since-ukraine-war-started/2551798.

More recently, in January 2026, Germany expelled a Russian diplomat identified as a military intelligence officer accused of espionage tied to the conflict, with Moscow responding by expelling a German diplomat in a tit-for-tat move.[178]

These measures create symbolic and political costs by isolating Moscow diplomatically and highlighting international condemnation of Russia's hybrid operations. While most expulsions have not been tied to specific cyber incidents, they contribute to raising costs for Russia's intelligence apparatus – which integrates cyber operations with traditional espionage and influence campaigns – and complicate the conduct of future hostile operations. Actions taken under disruption and cost imposition form part of a cumulative signalling strategy: repeated public attributions, coordinated sanctions, synchronized diplomatic statements, arrests and prosecutions are intended to communicate resolve and impose reputational costs on Russia and its proxies. Although the effectiveness of individual measures may be limited, their accumulation over time can have a deterrent effect and shape adversary perceptions of risk and consequence.

C. Deterrence and its limits

There is credible evidence that coordinated law enforcement can generate short-term deterrence effects against cybercriminal and proxy actors, though these effects remain uneven. Analysts of cyber deterrence have distinguished between deterrence by denial – making attacks less likely to succeed – and deterrence by punishment, through imposing costs after the fact. The measures discussed in this section operate primarily through the latter mechanism, with the limitations that punishment-based deterrence is most effective when costs imposed are visible, credible and sufficiently severe to alter the cost–benefit calculations of potential actors.[179]

Following Operation Cronos – the multinational operation led by the UK National Crime Agency (NCA), US Department of Justice (DOJ) and Europol – the LockBit ransomware group's core infrastructure was seized, internal data exposed and key associates indicted; these measures significantly degraded the group's operational capacity and reputation in early 2024. Security analysts assessed that the operation undermined LockBit's trust relationships with affiliates by demonstrating that participation carried elevated legal risk, even for actors operating outside Western jurisdictions.[180]

More directly, the above-mentioned arrest and extradition of Victoria Eduardovna Dubranova from a third country to the US for her alleged role in supporting pro-Russian cyber operations – including activity linked to NoName057(16)

---

178 Connor, R. (2026), 'Germany expels Russian diplomat over spying case', Deutsche Welle, 22 January 2026, https://www.dw.com/en/germany-expels-russian-diplomat-summons-ambassador-over-espionage-case/a-75609339; Reuters (2026), 'Russia expels German diplomat, accuses Berlin of "spy mania"', Reuters, 5 February 2026, https://www.reuters.com/world/russia-expels-german-diplomat-tit-for-tat-move-2026-02-05.
179 Nye, J. S. (2017), 'Deterrence and Dissuasion in Cyberspace', *International Security*, 41(3), pp. 44–71, https://direct.mit.edu/isec/article/41/3/44/12147/Deterrence-and-Dissuasion-in-Cyberspace.
180 Burgess, M. (2024), 'A Global Police Operation Just Took Down the Notorious LockBit Ransomware Gang', *Wired*, 20 February 2024, https://www.wired.com/story/lockbit-ransomware-takedown-website-nca-fbi.

and CyberArmyofRussia_Reborn – provided a concrete demonstration that individuals suspected of involvement in Russian-aligned proxy cyber activity may face personal legal consequences beyond Russia's borders. This case[181] materially challenges assumptions about geographic safe havens, and plausibly increases perceived risk among opportunistic or peripheral participants. In parallel, Europol-coordinated actions against NoName057(16) included public warnings and direct outreach highlighting criminal liability, which authorities assessed as contributing to some disengagement among lower-commitment volunteers, even if precise attrition levels remain unverified.

At the same time, the limitations of deterrence are substantial and persistent. Despite repeated disruptions, pro-Russian hacktivist activity has continued, with DDoS campaigns against NATO-aligned states remaining a recurrent feature of the threat landscape. LockBit re-established an online presence after the 2024 takedown; this has been cited as evidence that ransomware ecosystems can absorb infrastructure losses and reconstitute themselves quickly.[182] However, LockBit's credibility among affiliates collapsed, its activity levels dropped sharply, and the group has shown little meaningful operational recovery. The more precise conclusion is that Operation Cronos deterred the activity rather than eliminating the actor – a distinction that matters for how we measure the success of disruption operations. Nevertheless, new or rebranded pro-Russian hacktivist entities have continued to emerge, indicating a low barrier to entry and a surplus of motivated participants willing to replace disrupted actors. This suggests that deterring individual groups, while valuable, does not on its own remove the structural conditions that make proxy recruitment possible.

There is no publicly available evidence that cumulative disruptions, indictments or sanctions have altered Russia's strategic reliance on cyber proxies.

Most significantly, there is no publicly available evidence that cumulative disruptions, indictments or sanctions have altered Russia's strategic reliance on cyber proxies. Western governments have sanctioned GRU officers and Russian cyber units, and have publicly attributed state-directed malicious activity to Russia, yet Russia has continued to tolerate – and in some cases indirectly enable – criminal and hacktivist actors that advance its strategic objectives while preserving plausible deniability. The persistence of proxy activity suggests that, from Moscow's perspective, the operational and political benefits of cyber proxies outweigh the cumulative costs imposed by international pressure. This limits the strategic deterrent value of current countermeasures.

---

181 Dubranova has pleaded not guilty to all charges. As of 24 March 2026, as this paper was being finalized for publication, legal proceedings remained in progress.
182 Perera, D. (2024), 'Ransomware Operation LockBit Relaunches Dark Web Leak Site', GovInfoSecurity, 24 February 2024, https://www.govinfosecurity.com/ransomware-operation-lockbit-relaunches-dark-web-leak-site-a-24442.

05 Recommendations: the case for strategic coherence

Existing tools – disruption, sanctions, investigation and prosecution – are sufficient in principle to hold cyber proxies accountable. What is missing is coordination. This chapter sets out concrete recommendations for moving from fragmented tactical responses to strategically coherent, sustained pressure.

Ukraine and its allies possess the tools to hold cyber proxies accountable – disruption capabilities, sanctions frameworks, prosecution authorities. The challenge is not inventing new mechanisms but coordinating existing ones so they reinforce rather than undermine each other. Moving from tactical disruption to strategic degradation of cyber proxies requires integrating existing tools and focusing efforts where they matter most – critically, it requires cultivating the political will to treat multi-dimensional, coordinated response as a priority.

This chapter organizes its recommendations around a hierarchy of proposed actions. It distinguishes between (A) core strategic levers, (B) strategic amplifiers and (C) enablers. Core levers create immediate operational friction and impose costs that cannot easily be evaded. Amplifiers magnify and sustain the effects of these levers across legal, operational and reputational dimensions. Enablers build the institutional and normative foundations for long-term effectiveness. This framing reflects both the political realities facing states seeking to tackle cyber proxy activities and the recognition that not all measures carry equal weight. Put another way, when resources and political bandwidth are finite, prioritization matters.

A. Core strategic levers: actions that directly degrade proxy capacity

In the first instance, we argue, governments and institutions seeking to tackle cyber proxies need to apply core levers as follows:

1. Target enabling ecosystems, not just individual actors

Effective disruption of proxy operations requires focusing on the infrastructure and supply chains that enable them: cryptocurrency exchanges facilitating payments, hosting providers enabling command-and-control infrastructure, technology suppliers providing tools, etc. Focusing on infrastructure rather than solely on individual actors is particularly effective because the same platforms and services often support cyber and information operations and other actors.[183] While not conceptually new, ecosystem-level targeting has rarely been applied systematically or at scale.[184] Achieving scale and consistency requires measures targeting the following entities:

- So-called 'bulletproof hosting' providers (internet hosting services that deliberately ignore takedown requests and legal demands, enabling proxy operations to persist and other malicious and illegal activity) and virtual private network (VPN) services that enable proxy operations;
- Cryptocurrency exchanges and mixers that facilitate payment flows;
- Domain registrars and content delivery networks (CDNs) that support cyberattacks and information campaigns; and
- Technology suppliers that provide malware-as-a-service or offensive tools.

Critical to this is the need to **impose costs on enablers.** Sanctions designations, prosecutions and public exposure should target not just proxy operators but the infrastructure providers, payment processors and technology suppliers that make proxy operations scalable. States should coordinate such designations multilaterally (see also Recommendation A2, below) to prevent targets from simply relocating to permissive jurisdictions. This requires differentiating between jurisdictions that harbour proxy infrastructure through lack of capability and those that do so deliberately – a distinction developed further in Recommendation C1.

183 CyberPeace Institute (2026), 'Why look at infrastructure in nexus operations?', 5 February 2026, https://cyberpeaceinstitute.org/news/why-look-at-infrastructure-in-nexus-operations.
184 The Ransomware Task Force (RTF), convened by the Institute for Security and Technology (IST) in 2021, produced 48 recommendations centring on disrupting ransomware-enabling infrastructure, including cryptocurrency exchanges and hosting providers. Ransomware Task Force (2021), 'Combating Ransomware: A Comprehensive Framework for Action', Institute for Security and Technology, 21 April 2021, https://securityandtechnology.org/virtual-library/report/combating-ransomware-a-comprehensive-framework-for-action.

2. Create standing mechanisms for rapid multilateral coordination of sanctions

Coordinated sanctions multiply pressure by closing safe havens. The EU's June 2024 cyber sanctions demonstrate the potential for multilateral action, but current practice remains largely ad hoc. Moving from reactive to systematic responses requires institutionalizing the coordination infrastructure before the next major incident, not during it. Willing partners – at minimum the US, the UK, the EU, Australia, Canada and Japan – should establish a permanent cyber sanctions coordination cell with a mandate to take the following measures:

- **Pre-position designation packages** for known proxy networks, infrastructure providers and enablers of cyber-enabled operations, allowing sanctions to be activated quickly rather than constructed from scratch in a crisis. Pre-positioning would not remove the requirement for case-by-case ministerial review and legal assessment at the point of decision; rather, it would ensure the necessary evidentiary groundwork is already in place, facilitating faster adoption when the threshold for designation is met.
- **Share attribution assessments, legal analysis and supporting intelligence** through secure channels to enable faster, better-coordinated responses.
- **Develop interoperable evidentiary standards** for designations that accommodate different legal systems, while preserving enforceability across jurisdictions.
- **Harmonize national cyber sanctions frameworks across participating jurisdictions** where legal gaps or inconsistencies exist. Like-minded states should ensure their existing frameworks can accommodate coordinated cyber-specific listings, enabling full participation in rapid multilateral actions.
- **Establish clear activation triggers and decision-making procedures**, so that participating governments agree in advance on the threshold and process for deploying pre-positioned packages – since this is where sovereign legal differences are most likely to create friction.

By institutionalizing pre-authorized response pathways and shared operational infrastructure, this mechanism would allow sanctions to function as a rapid, integrated instrument of collective cyber deterrence rather than as a reactive or symbolic measure.

3. Integrate evidence sharing with broader disruption strategies

Bilateral and multilateral evidence-sharing mechanisms – including MLATs, the Budapest Convention framework and joint investigation teams – have enabled successful prosecutions, as demonstrated by operations targeting NoName057(16), LockBit and other proxy networks. However, the strategic gap does not lie with cooperation mechanisms themselves; rather, it is the persistent disconnect between law enforcement, sanctions authorities, intelligence agencies and diplomatic services – within and between governments – in integrating evidence collection with sanctions, operational disruption and diplomatic pressure to generate compounding effects.

When evidence sharing operates independently of other response tools, its impact is limited. Criminal investigations that proceed without coordination with sanctions authorities may inadvertently alert targets before asset freezes can be imposed. Infrastructure takedowns conducted without preserving evidence for prosecution risk wasting opportunities for criminal accountability.

To achieve strategic integration, the relevant authorities and agencies need to:

— **Coordinate timing across tools**. This means aligning evidence collection with sanctions designations and operational disruptions to ensure that criminal investigations, technical takedowns and financial measures reinforce rather than undermine each other. Operation Cronos demonstrated the benefit of sequencing actions to maximize their legal and strategic effects.

— **Expand direct judicial cooperation**. This will entail building on frameworks such as the EU's e-Evidence Regulation and bilateral agreements under the US CLOUD Act to enable authorities to request data directly from providers across borders, while respecting privacy and legal safeguards.

— **Formalize rapid-response protocols.** Policymakers should establish pre-agreed procedures for high-priority cases involving critical infrastructure or active campaigns, ensuring that law enforcement, intelligence agencies and private sector partners act in a synchronized, rapid and legally compliant manner rather than relying on ad hoc coordination during crises.

B. Strategic amplifiers: measures that magnify pressure

Like-minded states, working through national authorities and multilateral bodies such as Europol and Eurojust, should take the following steps to amplify the effects of the above-mentioned core levers:

1. Coordinate operational disruption campaigns

Current disruption efforts often treat each incident as isolated. Infrastructure is seized, domains are taken down, but proxies regroup and reconstitute themselves quickly using alternative providers. A shift to 'campaign-based' disruption would enable one-off actions to be replaced with sustained pressure targeting the same proxy network across multiple dimensions simultaneously. Policymakers should:

— **Focus campaigns on high-value targets.** This means prioritizing proxy networks that enable multiple types of operations (cyber and information operations) or that support critical Russian strategic objectives, rather than attempting to disrupt every proxy operation globally.

— **Target shared infrastructure.** This will entail identifying hosting providers, CDNs and domain registrars used by proxies for cyber and information operations. Takedowns of shared infrastructure should be coordinated to generate compounding effects, the aim being to simultaneously degrade offensive cyber capabilities and dismantle influence networks.

— **Deny reconstitution, not just access**. Takedowns of proxies should be carefully sequenced in coordination with sanctions targeting infrastructure providers. Technical disruptions should be complemented with legal action (civil suits, criminal prosecution) that impose lasting consequences on facilitators. Publicizing disruptions would also help to increase reputational costs to cyber proxies and their sponsors.

Across all these measures, the cognitive dimension of disruption deserves explicit attention. Technical takedowns achieve their greatest strategic value when they are designed to generate psychological and organizational friction within adversary networks – eroding trust among affiliates, undermining leadership credibility, and creating doubt about the reliability of tools and partners. Operation Cronos (see Table 3) illustrates this well: the operation's most lasting effect was not the seizure of infrastructure but the reputational collapse it triggered within the LockBit ecosystem, which proved difficult to reverse.

Disruption campaigns should be designed from the outset with this signalling dimension in mind: identifying the pressure points where targeted interventions can generate disproportionate and compounding effects, and ensuring that operations are visible, attributed and sequenced to maximize organizational friction rather than being treated as isolated technical events.

Finally, these tools have structural limits – particularly where proxies operate from safe havens beyond the reach of law enforcement. In such contexts, some states have publicly acknowledged that offensive cyber capabilities form part of their national security toolkit. Whether and how such capabilities should be integrated into the coordinated accountability frameworks recommended here – and under what legal and oversight conditions – is a question that deserves serious attention, even if it remains politically sensitive.[185]

2. Establish structured public–private engagement frameworks

Technology companies control much of the infrastructure that proxies exploit, but the former's cooperation with governments often remains ad hoc, inconsistent and hampered by concerns about liability, resource constraints, and conflicts between security obligations and user privacy commitments. Formalizing engagement would transform reactive coordination into predictable partnerships with clear roles and mutual expectations – combining incentives with binding obligations.

Policymakers need to **define clear expectations for infrastructure providers.** This implies the following actions:

— Technology companies and infrastructure providers should be required to report proxy activity detected on their platforms, and preserve evidence for lawful investigations in a timely manner.

185 This question is beyond the scope of the present paper but warrants dedicated analysis, particularly as more states publicly acknowledge offensive cyber as part of their national security toolkit.

- Where companies detect active proxy campaigns, they should have pre-agreed protocols for coordinating with law enforcement rather than acting unilaterally – to ensure that technical disruption does not inadvertently compromise ongoing criminal investigations or destroy evidence needed for prosecution.
- Governments should explore the possibility of expanding mandatory reporting requirements for cyber incidents, scaled proportionately to organizational size. Current obligations – focused primarily on data theft and personal data breaches – may not adequately capture the full range of hostile cyber activity relevant to proxy operations. Governments should assess whether reporting obligations should be extended to include suspected espionage and unauthorized access to government and corporate networks and systems. Key points to address include: the evidentiary threshold that would trigger reporting; whether reports should flow to regulatory bodies or directly to law enforcement and intelligence agencies; how to manage disclosure risks; and what liability protections companies would require to participate in good faith. Structured dialogue with industry on the design of reporting procedures could ensure that requirements are technically workable and consistently applied across jurisdictions. It will be important to develop operational definitions of 'espionage' and 'unauthorized access' in a corporate context. Existing mandatory reporting frameworks among like-minded states offer useful starting points.

In addition, work on establishing structured public–private engagement needs to:

- **Balance obligations with safeguards**. This means ensuring frameworks respect human rights obligations, particularly regarding content moderation, data sharing and user privacy. It also means preventing inappropriate delegation of state authority to private companies for decisions on attribution or designation.
- **Address non-compliance**. For companies that refuse to cooperate or that persistently enable proxy infrastructure, states should consider consequences such as loss of government contracts, public disclosure of non-cooperation or, in serious cases, placement on a sanctions' list. At the same time, governments should prioritize cooperation with willing partners rather than attempting to compel universal participation – building coalitions of cooperative providers creates competitive pressure on holdouts.

Effective public–private engagement would help to transform companies from passive infrastructure providers into active contributors to collective defence, amplifying the effects of government actions through the corporate sector's unique capabilities and visibility into proxy operations.

C. Enablers: building foundations for long-term effectiveness

To sustain long-term effectiveness and reinforce the institutional foundations on which core levers and amplifiers depend, like-minded states should take the following steps:

1. Strengthen multilateral coordination infrastructure

Effective coordination across states and agencies is essential, but current mechanisms have limits. Organizations such as Europol, Interpol and Eurojust provide valuable avenues for collaboration, and schemes like the Counter Ransomware Initiative demonstrate potential for accelerated crisis response. However, real-time operational coordination is currently limited, domestic legal frameworks vary, and uneven resourcing creates gaps in capability that adversaries exploit.

To address these constraints, states should:

- **Enhance law enforcement cooperation** through Europol, Interpol, the EU SIRIUS network and Eurojust, ensuring agencies can share intelligence securely and coordinate responses in real time.
- **Invest in training and resources** to enable joint investigations and rapid operational coordination, underpinned by domestic legislation that explicitly permits such activities.
- **Ratify pending international instruments** that expand compatible legal frameworks for evidence sharing, namely: the UN Convention against Cybercrime and Second Additional Protocol to the Budapest Convention. While these instruments will not solve coordination challenges alone, they would expand the base of countries with aligned legal authorities for obtaining electronic evidence across borders.
- **Work towards common attribution standards** and shared frameworks for when and how to respond. While revisions to the Articles on State Responsibility are unlikely in practice, Track 1.5 dialogues – bringing together government officials, tech companies, researchers and civil society – can explore whether common methodologies are feasible while protecting intelligence sources.
- **Differentiate between inadvertent and deliberate safe havens.** States that harbour proxy infrastructure because they lack capability require a fundamentally different response from those that do so deliberately. For the former, targeted capacity-building support should be provided.

2. Sustain ecosystem pressure through multilateral and minilateral initiatives

While recommendations A1 and B1 mostly focus on directly targeting specific enabling infrastructure providers through sanctions and takedowns, sustained pressure requires multilateral frameworks that coordinate such actions over time and expand them globally. The Pall Mall Process and Counter Ransomware Initiative, for example, offer early models for how standing platforms can constrain enabling ecosystems beyond individual operations.

These initiatives become strategically coherent when they:

- **Connect to accountability mechanisms**. This ensures findings feed directly into sanctions regimes, criminal prosecutions and diplomatic pressure rather than operating as standalone research or dialogue forums.
- **Expand geographic participation**. Bringing in countries that currently lack comprehensive cyber sanctions or prosecution frameworks would create broader coverage against jurisdictional arbitrage, and would make it easier to close the safe havens that proxy networks systematically exploit.
- **Develop shared standards for designating persistent threat actors and harbouring states**. Frameworks analogous to those identifying 'state sponsors of terrorism' could be developed for use against states that persistently enable proxy ecosystems or harbour proxies. This would create a legal and diplomatic basis for graduated consequences.
- **Learn from adjacent international law frameworks**. Instruments addressing mercenaries, foreign fighters and transnational organized crime offer relevant precedents for connecting criminal, diplomatic and economic responses in ways that the current cyber accountability architecture has not yet replicated.

3. Build societal resilience and normative frameworks

Societal resilience reinforces the long-term effectiveness of action to combat cyber proxies by reducing their operational space and public tolerance for malicious activity. Increasing resilience requires action across three mutually reinforcing layers:

Public awareness and education

- States should promote media literacy programmes addressing influence operations, deepfakes and coordinated inauthentic behaviour.
- States should connect public education to accountability strategies, building understanding of government responses and political support for sustained pressure.

Government transparency about threats

- States should expand the toolkit through which they communicate the threat landscape – this should go beyond reactive advisories to include regular published bulletins, formal cyber threat-level systems analogous to terrorism threat levels, and more aggressive use of indictments as transparency instruments.
- More states should emulate the practice of publicly exposing Russian cyber interference in democratic processes and developing detailed threat actor profiles. This was demonstrated by the UK's public attribution of GRU cyber and hybrid operations,[186] and by the joint technical advisory on Sandworm/GRU Unit 74455 issued by the UK, US, Canadian and Australian cybersecurity agencies.[187] Equally instructive is the US practice of unsealing criminal indictments as transparency instruments, which simultaneously exposes threat actor tradecraft, signals intelligence capabilities, and creates reputational and legal costs for named individuals – making it one of the highest-impact public attribution mechanisms available to governments.[188]

Dedicated institutional capacity

- Governments should establish focused teams for hybrid threat response, coordinating law enforcement, intelligence and diplomatic functions to ensure responses are integrated rather than siloed. The UK Foreign, Commonwealth and Development Office's establishment of the Cyber, Information and Tech Threats Directorate (CITT) reflects this approach, demonstrating recognition that sustained institutional capacity is necessary for strategic and coordinated interventions.[189]

---

186 Foreign, Commonwealth and Development Office, Home Office, Cabinet Office and National Cyber Security Centre (2025), 'Profile: GRU Cyber and Hybrid Threat Operations', policy paper, 4 December 2025, https://www.gov.uk/government/publications/profile-gru-cyber-and-hybrid-threat-operations/profile-gru-cyber-and-hybrid-threat-operations.
187 Cybersecurity and Infrastructure Security Agency, Federal Bureau of Investigation and National Security Agency (2025), 'Pro-Russia Hacktivists Conduct Opportunistic Attacks Against US and Global Critical Infrastructure', joint cybersecurity advisory AA25-343A, 9 December 2025, https://www.cisa.gov/news-events/cybersecurity-advisories/aa25-343a.
188 U.S. Department of Justice (2020), 'Six Russian GRU Officers Charged in Connection with Worldwide Deployment of Destructive Malware and Other Disruptive Actions in Cyberspace', press release, 19 October 2020, https://www.justice.gov/archives/opa/pr/six-russian-gru-officers-charged-connection-worldwide-deployment-destructive-malware-and; and Federal Bureau of Investigation (2020), 'GRU Hackers: Destructive Malware and International Cyber Attacks', wanted notice, October 2020, https://www.fbi.gov/wanted/cyber/gru-hackers-destructive-malware-and-international-cyber-attacks.
189 Foreign, Commonwealth and Development Office (2025), 'Written evidence submitted by the Foreign, Commonwealth and Development Office (DIS0029)', written evidence to the House of Commons Foreign Affairs Committee inquiry into 'Disinformation diplomacy: How malign actors are seeking to undermine democracy', https://committees.parliament.uk/writtenevidence/138112/pdf.

4. Bridge UN cyber governance and cybercrime processes

Russia's use of proxies deliberately blurs the line between state-sponsored operations and criminal activity, complicating efforts to establish accountability under existing frameworks. The UN addresses the issues through parallel but disconnected processes: one focused on cyber governance and norms (First Committee, Global Mechanism on ICT Security); and one dedicated to cybercrime (Third Committee, UN Convention against Cybercrime). Bridging these tracks could strengthen accountability in respect of proxy operations.

However, such a proposal might meet political and institutional resistance. Governments have historically and deliberately kept cyber governance and cybercrime processes separate, concerned that connecting them would complicate attribution standards, blur the line between criminal and state responsibility, and create unwanted precedents in each forum. That resistance deserves acknowledgment. However, the rationale for strict separation has substantially weakened: the UN Convention against Cybercrime is now agreed, and the OEWG has transitioned into a permanent mechanism. The institutional landscape has changed sufficiently to revisit whether continued separation serves accountability or merely entrenches impunity.

In this context, we advocate the establishment of the following bridging mechanisms:

- Like-minded states should establish joint working sessions between First and Third Committee focal points during UN cyber meetings to identify overlapping issues (e.g., how cybercrime treaty implementation relates to due diligence obligations under the Framework for Responsible State Behaviour in Cyberspace).
- They should also task national delegations to coordinate across both processes, ensuring cybercrime prosecutions inform discussions of state due diligence obligations and vice versa.
- Relevant UN agencies such as the UN Institute for Disarmament Research (UNIDIR) should commission joint studies examining how states' obligations to prosecute cybercrime (Third Committee focus) intersect with obligations to prevent territory from being used for malicious cyber operations (First Committee due diligence principle).

This integration would help address the current problem of proxy operations falling between governance frameworks: too state-linked to be treated as pure crime, yet too criminal to be clearly attributable as state action.

Table 4. Summary of recommendations and a hierarchy of actions

A. Core strategic levers: actions that directly degrade proxy capacity

1	**Target enabling ecosystems, not just individual actors** Sanctions and prosecutions should target enabling hosting providers, cryptocurrency exchanges and technology suppliers – not only proxy operators.
2	**Create standing mechanisms for rapid multilateral sanctions coordination** A permanent cyber sanctions coordination cell (consisting of representatives from the US, the UK, the EU, Australia, Canada and Japan) should be set up, with pre-positioned designation packages and agreed activation triggers.
3	**Integrate evidence-sharing with broader disruption strategies** Criminal investigations, technical takedowns and financial measures should be aligned so they reinforce rather than undermine each other.

B. Strategic amplifiers: measures that magnify and sustain pressure

1	**Coordinate operational disruption campaigns** Law enforcement, intelligence agencies and other relevant authorities should shift from one-off takedowns to sustained campaigns targeting proxy networks across multiple dimensions. Operations should be designed to generate organizational friction among cyber proxies and their affiliates, and to prevent disabled or disbanded proxies from regrouping and reconstituting their operations.
2	**Establish structured public–private engagement frameworks** Governments and regulators should formalize reporting obligations and disruption protocols with technology companies. Governments should establish liability protections for good-faith cooperation, with non-compliance addressed through regulatory consequences.

C. Enablers: building foundations for long-term effectiveness

1	**Strengthen multilateral coordination infrastructure** Governments should enlarge and extend cooperation through Europol, Interpol and Eurojust. States should also ratify the UN Convention against Cybercrime and the Second Additional Protocol to the Budapest Convention on Cybercrime, and should work towards common attribution standards.
2	**Sustain ecosystem pressure through multilateral and minilateral initiatives** States and policymakers should use multilateral and minilateral frameworks to coordinate sustained pressure on proxy ecosystems. This would help to expand the geographic reach of policy responses, and close jurisdictional loopholes.
3	**Build societal resilience and normative frameworks** Governments should build media literacy programmes, formal cyber threat-level systems, and dedicated institutional capacity for hybrid threat response.
4	**Bridge UN cyber governance and cybercrime processes** Like-minded states should connect different UN cyber processes through joint working sessions and coordinated national delegations.

States and institutions should prioritize recommendations A1–A3 when resources are limited – core levers create the foundation for amplifiers and enablers to take effect.

06 Conclusion

Russia's cyber proxy campaign against Ukraine and the West has exposed a fundamental gap between tactical capability and strategic coherence in Ukraine's allies. Closing that gap does not require new tools or perfect consensus – it requires the political will to coordinate what already exists.

The recommendations above demonstrate that strategic coherence in the West's battle against Russian cyber proxies – or indeed against other hostile states using cyber proxies both in conflict and in peacetime – is achievable without awaiting universal or domestic institutional reform or perfect international consensus. It can be built incrementally through deliberate prioritization: core strategic levers that directly degrade proxy capacity; strategic amplifiers that multiply pressure once foundational actions are engaged; and enablers that create conditions for long-term effectiveness.

This hierarchy matters. States that treat all measures as equally urgent risk diffusing effort across initiatives that cannot succeed in isolation. Core levers create operational friction that proxies cannot easily evade. Amplifiers compound that pressure across multiple dimensions simultaneously. Enablers sustain effectiveness over time. Together, they transform isolated functional responses into elements of unified accountability frameworks where attribution leads to consequences, where different tools reinforce rather than undermine each other, and where democratic states demonstrate institutional capacity for sustained collective action. Where resources are limited, we argue that states should prioritize Recommendations A1–A3 (i.e. core strategic levers) as this will create the foundation necessary for amplifiers and enablers to generate sustained impact.

Fragmentation is not an inevitability. It can be overcome by states and institutions prioritizing coordination. Recent developments and experience – from the operation to disable LockBit to multilateral EU sanctions coordination to emerging public–private frameworks – all demonstrate what becomes possible when institutional silos are bridged and actions are synchronized. These are not isolated successes but proof of concept: strategic coherence is feasible when deliberate institutional design is combined with sustained political commitment.

The question is not whether strategic coherence is achievable, but whether democratic governments will prioritize it alongside other demands. States face real constraints: ongoing crises requiring immediate attention; limited budgets; and competing policy priorities. These challenges are significant, yet they do not diminish the need for coordinated action. Continued fragmentation of the response to cyber proxy activity hands a lasting advantage to adversaries who face fewer comparable coordination difficulties. In a domain in which geopolitical power is increasingly exercised through proxies operating in grey zones, this remains a significant strategic vulnerability. States that implement the measures recommended in this paper will demonstrate that democratic governments can sustain coordinated, effective responses to proxy threats – denying adversaries the strategic advantage fragmentation currently provides.

About the authors

Joyce Hakmeh is an associate fellow at Chatham House and former deputy director of the institute's International Security Programme. She is also a senior associate at Oxford Information Labs and sits on the boards of the Global Cyber Alliance and Common Good Cyber. She served as co-editor and then commissioning editor of the *Journal of Cyber Policy*, helping drive the journal's growth into one of Taylor & Francis's fastest-expanding policy titles. Her work is widely published, spanning cyber governance, emerging technology risk, geopolitics and international security.

Joyce has played a central role in international cyber diplomacy, leading Chatham House's contributions to UN cyber negotiations. She convened and chaired the UK–China Cyber & Technology Track 1.5 Dialogue, facilitating critical exchanges on sensitive technology and security issues.

Earlier in her career, Joyce worked in international development and humanitarian policy with multilateral organizations including the UN Development Programme and the IFRC. She holds a master's degree in international law from SOAS, University of London.

Harriet Moynihan is head of accountability in international law at the Oxford Institute of Technology and Justice in the Blavatnik School of Government, University of Oxford. Harriet's work focuses on accountability for malicious cyber operations and on the use of technology, including AI tools, to strengthen accountability processes.

Harriet is also an associate fellow in the International Law Programme at Chatham House (of which she was formerly the director) and a research affiliate at the Oxford AI Governance Initiative of the Oxford Martin School, University of Oxford. Harriet previously worked for eight years as a legal adviser in the UK's Foreign & Commonwealth Office, and prior to that practised as a competition lawyer at the international law firm Clifford Chance LLP.

Dr Nayana Prakash is a research fellow in the International Security Programme at Chatham House and served as an associate editor of the *Journal of Cyber Policy*. She holds a PhD from the Oxford Internet Institute, where her research focused on digital platforms in India and creative uses of technology in the region.

Nayana's primary expertise is in technology governance in India and the geopolitics of technology in the Global South. She has written and researched widely on issues relating to dis- and misinformation, narrative manipulation on social media, AI in the workplace, and cybersecurity for vulnerable groups.

Acknowledgments

The authors would like to thank the participants in the workshop, held in November 2025 under the Chatham House Rule, who gave generously of their time and provided valuable insights. Particular thanks are due to Tim Stevens, Chris Painter, Ciaran Grant, Heli Tiilmaa-Klaar, Elizabeth Wilmshurst, Russell Buchan and the anonymous peer reviewers for their comments on this paper, and to Jake Statham for editing the paper. The views expressed in the paper are the sole responsibility of the authors. Chatham House is grateful to Global Affairs Canada, which gave support for this project.

Cover image: Multiple-exposure illustration of Ukrainian flag and binary code on screen, 2022.
Photo credit: Copyright © Jakub Porzycki/NurPhoto/Getty Images

ISBN 978 1 78413 677 2
DOI 10.55317/9781784136772

Cite this paper: Hakmeh, J., Moynihan, H. and Prakash, N. (2026), *Holding state-sponsored hackers and other cyber proxies to account: Lessons from tackling proxies in Russia's war on Ukraine*, Research Paper, London: Royal Institute of International Affairs, https://doi.org/10.55317/9781784136772.

This publication is printed on FSC-certified paper.
designbysoapbox.com

Independent thinking since 1920

CHATHAM HOUSE

The Royal Institute of International Affairs
Chatham House
10 St James's Square, London SW1Y 4LE
T +44 (0)20 7957 5700
contact@chathamhouse.org | chathamhouse.org

Charity Registration Number: 208223