Norway Sweden Sverige EDNANNIA ASKOLD AND DIR NORWEGIAN-SWEDISH POOLED FUND ECONOMIC SECURITY COUNCIL of UKRAINE

Policy Brief

The Cyber Sanctions Gap: Building United Front

Executive Summary

The policy brief underscores the urgent need to strengthen global cyber sanctions in response to escalating cyber threats, particularly in hybrid warfare contexts in 2025. It highlights the increasing frequency of cyber attacks, with notable incidents targeting critical infrastructure, and examines sanctions imposed by the US, EU, UK, and Australia. Public-private partnerships are vital for effective cyber sanctions, leveraging private sector expertise in technology, open-source intelligence, and innovation to enhance threat detection and enforcement. To address new challenges, the brief proposes creating a unified online registry for cyber sanctions, enhancing multilateral coordination platforms, and shifting toward sectoral sanctions on advanced technologies. It advocates for directly targeting sponsoring states, using non-mirrored sanctions, and integrating cyber sanctions with offensive cyber operations and self-defense measures under international law. These steps aim to foster a cohesive, adaptive global response to cyber threats, ensuring accountability and resilience.

General Context & Overview of Recent Cyber Sanctions

The first two quarters of 2025 witnessed a marked acceleration in digital aggression. Check Point[1] [2] reports that the average number of cyber attacks per organization had seen a 47% and 21% increase versus Q1 and Q2 of 2024 respectively, signaling a structural upward shift in baseline threat exposure. Ransomware episodes grew at an even faster pace amounting to a 126% year-on-year (YoY) increase, with North America being the target of roughly 62% and Europe – 21% of those incidents.

Target-wise, Africa appeared at the top of the weekly attacks list in both quarters, followed by APAC and Latin America. Europe, however, while not the region with the highest attack volume, registered the largest YoY increase of 22%. The most targeted sectors came to be:

Education
(+71% Q1; +31% Q2)

Government
(+51% Q1; +26% Q2)

Telecommunications
(+94 Q1; +38% Q2)

Major cyber incidents swept through every critical sector, with Russia-, PRC- and Iran-linked and state-sponsored actors targeting critical infrastructure and government systems worldwide. This year has seen "...one of the most consequential cyber espionage breaches ... ever seen in the United States" with China's Salt Typhoon intrusion into the telecom networks[3];

1.https://blog.checkpoint.com/research/q1-2025-global-cyber-attack-report-from-check-point-software-an-almost-50-surge-in-cyber-threats-worldwide-with-a-rise-of-126-in-ransomware-attacks/

2.https://blog.checkpoint.com/research/global-cyber-attacks-surge-21-in-q2-2025-europe-experiences-the-highest-increase-of-all-regions/

3.https://www.theregister.com/2025/08/28/fbi_cyber_cop_salt_typhoon

significant ransomware attacks on European Airoports in September[4]; malicious cyber groups targeting SalesForse[5], healthcare[6], federal systems[7]...

In this environment, sanctions stand out as one of the few instruments capable of altering the cost–benefit calculus of state-directed or state-tolerated cyber aggression. Unlike purely defensive measures, coordinated sanctions project political attribution, impose reputational and material costs on hostile ecosystems, and function as a proxy for collective deterrence when military responses would be disproportionate. In essence, they convert digital disruption into economic and diplomatic pressure, transforming virtual aggression into real-world accountability.

Yet, in practice, the global cyber-sanctions architecture remains fragmented. In the first three quarters of 2025 the US[8], the EU[9], the UK[10], and Australia have collectively designated 40 individuals and 24 entities for cyber-related activities. Of those, only three individuals appear on both EU and UK lists – and the EU imposed its measures roughly seven months earlier. No other overlaps were recorded. What this reveals is structural incoherence in how jurisdictions define, attribute, and prioritize cyber threats.

The case of Garantex, a Russia-based cryptocurrency exchange, exemplifies this misalignment. The entity was sanctioned by the United States under its cyber-related program in August 2025, listed by the UK under Russia-related measures as early as April 2022, and designated by the EU under Ukraine-related sanctions in February 2025[11]. Despite targeting the same actor, the programs cite different justifications and timing, with no official explanation in the lists for this variation. There is another bottleneck, and it is the inconsistent listing and opaque attribution. Ukraine's national sanctions registry, for instance, often omits detailed reasoning or evidentiary bases for designations, limiting interoperability and legal clarity.

For that matter, the uneven pace and rationale of cyber-related designations across major Western jurisdictions illustrate the absence of a unified sanctions doctrine in the digital domain. While all four sanctioning powers nominally pursue deterrence of hostile cyber operations, their measures tend to emerge reactively and with significant fragmentation – some housed under "Russia," others under "cyber," "human rights," or "Ukraine" and mostly with virtually no coordination.

Nonetheless, several patterns are discernible. Across jurisdictions, the predominant restrictive measure remains the asset freeze, applied in all cyber-related designations. This preference reflects the limited toolkit available for targeting digital aggressors, as financial and transactional restrictions remain the most enforceable form of extraterritorial pressure. The vast majority of sanctioned actors originate from Russia, China, and Southeast Asia, underscoring the geopolitical concentration of offensive cyber capacity and the attribution confidence that tends to accompany campaigns emanating from these regions. Additionally, most of the Russian individuals are the associates of the Main Directorate of the General Staff of the Armed Forces of the Russian Federation (GRU).

Alas, the rationale behind these measures often lacks analytical precision. In most jurisdictions, sanctions announcements rely on citing "malicious cyber activity threatening national security or citizens". The US and the EU remain a notable exception. Their designations are accompanied by official and detailed press releases, often referencing specific threat groups, intrusion campaigns, or infrastructure components.

4.https://www.securityweek.com/european-airport-cyberattack-linked-to-obscure-ransomware-suspect-arrested/
5.https://cybernews.com/news/stellantis-jeep-dodge-automaker-data-breach-salesforce-shiny-hunters/
6.https://cybernews.com/news/pacific-healthworks-everest-ransomware-attack-la-perouse-data-leak-physician-groups/
7.https://www.nytimes.com/2025/08/12/us/politics/russia-hack-federal-court-system.html
8.https://home.treasury.gov/news/press-releases?title=cyber+&publication-start-date=&publication-end-date=
9.https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32025D0171
10.https://www.bvifsc.vg/sites/default/files/31jul25-uk-sanctions-update-cyber-russia-regime.pdf
11.https://www.opensanctions.org/entities/NK-XQyqxmZPMezqQiDeHoGQjf/

Role of the Public-Private Partnership

Sanctions and export controls related to cyber threats cannot be effectively developed or implemented without robust collaboration with the private sector. Private companies, particularly those in the technology and cybersecurity industries, possess critical expertise, resources, and real-time data that are essential for identifying and countering cyber threats. Governments rely on private sector innovation to track malicious actors, develop defensive technologies, and enforce sanctions effectively.

Civil society organizations and businesses have proven to be reliable partners in the development of traditional sanctions, as demonstrated by Ukraine's experience in countering Russian aggression. This collaboration has been pivotal in areas such as open-source intelligence (OSINT) investigations, private intelligence gathering, and ongoing monitoring of sanctioned entities. The success of these efforts highlights the need to scale up such practices to address cyber sanctions. By partnering with private entities, the state can access specialized skills and technologies that enhance its ability to track illicit cyber

activities, identify sanction evasion tactics, and strengthen enforcement mechanisms. Expanding these partnerships is critical to building a resilient sanctions framework that adapts to evolving cyber threats.

The private sector is equally indispensable in shaping regulatory approaches to sanctions and related tools, such as export controls and investment screening in high-tech industries. Private companies often operate at the forefront of technological innovation, giving them unique insights into the risks and opportunities associated with emerging technologies. Without their input, governments risk creating regulations that are either overly restrictive, stifling innovation, or too lax, failing to address vulnerabilities.

Ukraine has valuable experience in fostering public-private collaboration that can serve as a model. The National Sanctions Coalition, coordinated by the Economic Security Council of Ukraine, exemplifies how partnerships between the government, civil society, and businesses can drive sanctions policy forward. Additionally, the ESCU is working on launching the Trusted Tech Caucus in Ukraine's parliament, in collaboration with the Krach Institute for Tech Diplomacy at Purdue and the Association of People's Deputies of Ukraine. This initiative aims to engage the private sector in developing regulations for cutting-edge technologies, ensuring that policies are informed by industry expertise and aligned with global best practices.

Policy Recommendations

Recommendation 1:
Establish a Unified Online Registry for Cyber Sanctions

The establishment of a unified online registry for cyber sanctions is essential to enhance the effectiveness of international responses to cyber threats. Drawing lessons from existing sanctions regimes against Russia, such as those imposed by the EU and the US, consolidated registries have proven invaluable in enabling rapid verification of sanctioned entities. These systems allow stakeholders, including governments, businesses, and financial institutions, to quickly check whether an individual, organization, or entity is under restrictions, thereby reducing compliance risks and streamlining enforcement. In the context of cyber sanctions, a similar global registry would centralize information on designated cyber actors, making it easier to track and attribute malicious activities across borders.

Furthermore, a unified registry would facilitate better mapping of cyber threat groups, which often operate through proxies. By aggregating data from multiple jurisdictions, it would provide a comprehensive view of affiliations, tactics, and operational patterns, aiding intelligence sharing among allies. This is particularly crucial given the shared nature of cyber threats, where attacks on one nation can have spillover effects on others, such as disrupting critical infrastructure or stealing sensitive data. A centralized platform would promote consistency in designations and help prevent evasion tactics, like rebranding or relocating operations, that cybercriminals frequently employ.

In conclusion, implementing such a registry requires international collaboration to ensure data accuracy, privacy protection, and regular updates. Allies should prioritize interoperability standards to integrate existing national databases, fostering a collective defense mechanism.

Recommendation 2:
Enhance Effective Cooperation Through Synchronized Platforms

While joint statements on cyber sanctions demonstrate a commitment to collective action, the lack of synchronization across regimes undermines their impact. Different countries often impose varying levels of restrictions, leading to loopholes that malicious actors exploit. To address this, there is a pressing need to create dedicated platforms for ongoing coordination, such as multilateral forums or digital portals where allies can align their sanction lists, share evidence, and harmonize enforcement strategies.

Moreover, making restrictions more universal involves standardizing criteria for designations and penalties. For instance, adopting common thresholds for attributing cyber incidents could prevent discrepancies that allow offenders to seek safe havens in less stringent jurisdictions. These platforms could also facilitate real-time information exchange, enabling quicker responses to emerging threats. By fostering a collaborative environment, allies can pool resources for investigations and capacity-building, particularly for nations with limited cyber expertise.

Ultimately, effective cooperation demands political will and institutional support to overcome barriers like differing legal frameworks. Establishing joint task forces could institutionalize these efforts, leading to a more cohesive international front against cyber aggression. This synchronized approach would not only amplify the pressure on violators but also signal a united resolve to uphold cyber norms.

Recommendation 3:
Shift Toward Sectoral Sanctions on Advanced Technologies

Transitioning to sectoral sanctions is critical to limit authoritarian regimes access to cutting-edge technologies that fuel cyber attacks. Technologies such as cloud services, advanced networking tools, and data analytics platforms are often dual-use, enabling both legitimate operations and malicious cyber campaigns. By imposing broad restrictions on entire sectors, rather than targeting specific entities, sanctions can disrupt the supply chains that support state-backed hackers, thereby reducing their capacity to launch sophisticated intrusions like ransomware or espionage operations.

In addition, regulatory frameworks for emerging technologies like artificial intelligence (AI) must be integrated into these sanctions. AI systems can automate cyber threats, making them a strategic asset for adversarial states. Sanctions should be connected to export controls and investment bans on AI-related hardware and software, ensuring that authoritarian regimes cannot acquire or develop these capabilities unchecked. This proactive stance would prevent the proliferation of AI-driven threats and promote ethical global standards in technology development.

Overall, this shift requires careful calibration to minimize unintended economic impacts on global markets while maximizing security gains. By focusing on high-risk technologies, sectoral sanctions would serve as a powerful tool to curb cyber aggression and foster a safer digital landscape.

Recommendation 4:
Expand Sanctions and Attribution to Include States Directly

Sanctions and attribution efforts must extend beyond cyber groups to directly target sponsoring states, recognizing that many cyber operations are state-directed. While technical attribution focuses on digital forensics, such as IP traces or malware signatures, political attribution becomes relevant in multifaceted armed conflicts where cyber attacks are part of broader hybrid warfare. This dual approach allows for holding governments accountable, even when direct links are obscured through deniable proxies, thereby closing gaps in current regimes that often shield state actors.

Attributing responsibility to states enables more comprehensive sanctions, including diplomatic, economic, or travel restrictions that go beyond cyber-specific measures. For example, in cases where a cyber incident is linked to a state's intelligence apparatus, sanctions could freeze assets or ban officials from international forums. This broader scope deters escalation by making the costs of cyber aggression felt at the national level, encouraging restraint among potential aggressors.

To implement this effectively, allies should develop shared protocols for attribution, combining intelligence from multiple sources to build robust cases. This would enhance the legitimacy of sanctions and reduce the risk of misattribution. Ultimately, targeting states directly strengthens the international rule of law in cyberspace, promoting accountability and stability.

Recommendation 5:
Implement Non-Mirrored Sanctions in Response to Cyber Attacks

Sanctions imposed in response to cyber attacks should not be limited to mirroring the cyber domain; instead, they can encompass a wider array of restrictions on the offending state's rights and opportunities. This flexibility allows for asymmetric responses that target vulnerabilities in other sectors, such as finance, trade, or diplomacy, amplifying the punitive impact. For instance, a cyber intrusion on critical infrastructure could trigger sanctions on energy exports or cultural exchanges, disrupting the aggressor's broader interests without escalating to direct cyber retaliation.

This approach recognizes that cyber attacks often serve strategic goals beyond the digital realm, such as economic sabotage or political influence. By decoupling the response from the attack's nature, sanctions become a versatile tool in a nation's foreign policy arsenal, tailored to maximize deterrence while minimizing risks of mutual cyber escalation. It also allows for proportionate measures that align with international law, ensuring responses are justified and effective.

In practice, decision-makers should assess the context of each incident to select appropriate non-mirrored sanctions, consulting with allies for coordinated action. This strategy not only punishes the immediate offense but also signals that cyber aggression will invite multifaceted consequences, fostering a more secure global environment.

Recommendation 6:
Develop Autonomous Regimes for Cyber Sanctions with Cumulative Application

Cyber sanctions can operate as a standalone autonomous regime, distinct from other sanction frameworks, to address the unique nature of digital threats. This independence allows for specialized measures, such as blocking access to global networks or freezing cryptocurrency assets used by hackers, without intertwining them with unrelated geopolitical issues. An autonomous regime streamlines implementation, enabling rapid designations based on cyber-specific evidence and reducing bureaucratic hurdles in multi-domain conflicts.

However, when a cyber attack forms part of an armed or hybrid assault, these sanctions should be applied cumulatively alongside other restrictions. For example, if a cyber operation supports military aggression, it could trigger layered penalties under both cyber and conventional warfare regimes, compounding the pressure on the perpetrator. This cumulative approach ensures comprehensive coverage, preventing aggressors from compartmentalizing their actions to evade full accountability.

To balance these elements, international agreements should define triggers for autonomy versus integration, promoting clarity and consistency. Such a framework would enhance the adaptability of sanctions, making them a more potent instrument in countering evolving cyber-hybrid threats.

Recommendation 7:
Promote Joint Attribution to Strengthen Accuracy and Deterrence

Joint attribution processes significantly improve the precision in identifying perpetrators of cyber attacks, leveraging collective intelligence from multiple nations. By pooling technical data, such as malware samples and network logs, allies can corroborate findings and reduce errors that might arise from isolated analyses. This collaborative effort not only refines the evidence base but also builds a shared understanding of threat actors 'methodologies, enabling more targeted and effective countermeasures.

Moreover, joint attribution legitimizes subsequent actions, such as sanctions or diplomatic condemnations, by demonstrating international consensus. When multiple countries publicly attribute an attack, it undermines the aggressor's plausible deniability and amplifies the moral and legal weight of the response. This unity signals to potential offenders that cyber aggression will face a coordinated backlash, thereby enhancing deterrence and discouraging future incidents.

In fostering this practice, mechanisms like information-sharing hubs or joint cyber centers should be established to facilitate secure collaboration. Over time, joint attribution will contribute to norm-building in cyberspace, promoting transparency and accountability among states.

Recommendation 8:
Foster Better Collaboration with the Private Sector on Technology Non-Proliferation

Improved collaboration with the private sector is vital to prevent the spread of advanced technologies to authoritarian regimes that could enable cyber attacks. Companies in tech, telecom, and software industries hold key roles in supply chains and should adopt corporate responsibility standards to scrutinize exports and partnerships. This includes due diligence processes to identify risks of technology misuse, such as in surveillance or offensive cyber tools, thereby aligning business practices with global security interests.

Public-private partnerships can facilitate this through frameworks for sharing threat intelligence and best practices. Such synergy would help in preempting the acquisition of tools like AI algorithms or cloud infrastructure by malicious states, reducing the overall threat landscape.

Ultimately, this collaboration requires trust-building measures, including legal protections for shared data and joint working groups. By embedding corporate responsibility into the fight against cyber proliferation, allies can create a more robust barrier against authoritarian exploitation of technology, enhancing collective cyber resilience.

Recommendation 9:
Adapt Approaches to Private Military Companies Considering the Emergence of Cyber Mercenaries

The rise of cyber mercenaries — private actors hired for offensive cyber operations — necessitates a fundamental shift in how Private Military Companies (PMCs) are regulated. Traditionally focused on physical warfare, PMCs are increasingly involved in digital domains, blurring lines between state and non-state actors. This evolution demands updated international frameworks that explicitly address cyber activities. By recognizing cyber mercenaries as extensions of traditional PMCs, regulators can impose licensing requirements, oversight mechanisms, and accountability measures to prevent unregulated proliferation of cyber capabilities that could escalate conflicts.

Sanctions should be applied to PMCs that violate international law, including humanitarian norms, in cyberspace. For instance, if a PMC conducts indiscriminate cyber attacks affecting civilians — such as disrupting hospitals or water systems — it could face asset freezes, travel bans, or contract prohibitions. This approach aligns with principles from the Geneva Conventions, adapted to digital warfare, ensuring that cyber operations respect proportionality and distinction. Targeting non-compliant PMCs with sanctions would deter their involvement in illicit activities and pressure host states to enforce compliance, reducing the appeal of outsourcing cyber aggression.

Ultimately, this regulatory adaptation requires multilateral cooperation to define "cyber mercenary" and establish monitoring bodies. By integrating sanctions into a broader regulatory ecosystem, allies can mitigate risks posed by privatized cyber threats, fostering a more accountable and secure global cyber environment while upholding humanitarian standards.

Recommendation 10:
Combine Sanctions with Other Measures of Influence, Including Offensive Cyber Operations and Self-Defense

To maximize impact, cyber sanctions should be integrated with a spectrum of influence measures, creating a multifaceted strategy against aggressors. This includes diplomatic pressure, economic incentives for compliance, and information campaigns to expose malicious activities. By layering sanctions with these tools, responses become more adaptive and resilient, addressing not just immediate threats but also long-term behavioral change. For example, combining asset freezes with public attributions can amplify reputational damage, while economic aid to affected allies reinforces collective resilience.

A key element is transitioning toward offensive cyber operations as a complementary measure, conducted within legal bounds to disrupt adversaries capabilities proactively. Rather than relying solely on defensive postures, states should develop doctrines for targeted cyber countermeasures, such as neutralizing command-and-control servers used in attacks. This shift requires clear rules of engagement to avoid escalation, ensuring operations are proportionate and attributable only when strategically advantageous. Offensive actions, when paired with sanctions, can impose immediate costs, deterring future incidents more effectively than sanctions alone.

Furthermore, more active invocation of the right to self-defense under Article 51 of the UN Charter is essential in severe cyber incidents amounting to armed attacks. This provision allows for necessary and proportionate responses, potentially including kinetic measures if cyber threats cross thresholds. By framing cyber defenses within this legal framework, states can legitimize actions while coordinating with allies through bodies like NATO. This holistic approach—merging sanctions, offensives, and self-defense—strengthens deterrence, promotes international norms, and enhances global stability in an increasingly contested cyberspace.

Prepared by:

Dr. Ilona Khmeleva, Secretary of the Economic Security Council of Ukraine, Non-Resident Fellow at the George Washington University, khmeleva@escu.ua

Solomiia Vybranovska, Expert of the Economic Security Council of Ukraine, s.v@escu.ua

The recommendations were prepared in consultation with the Ministry of Foreign Affairs of Ukraine.

The policy brief is produced by the Economic Security Council of Ukraine with the support of the Askold and Dir Fund as a part of the Strong Civil Society of Ukraine – a Driver towards Reforms and Democracy project, implemented by ISAR Ednannia, funded by Norway and Sweden. The contents of this publication are the sole responsibility of the Economic Security Council of Ukraine and can in no way be taken to reflect the views of the Government of Norway, the Government of Sweden, and ISAR Ednannia.