A Global Policy Perspective on Offensive Cyberspace Operations

Gazmend Huskaj

November 2025

GCSP Policy Brief No.22

GCSP
Geneva Centre for Security Policy

Geneva Centre for Security Policy

The Geneva Centre for Security Policy (GCSP) is an international foundation that aims to advance global cooperation, security and peace. The foundation is supported by the Swiss government and governed by 55 member states. The GCSP provides a unique 360° approach to learn about and solve global challenges. The foundation's mission is to educate leaders, facilitate dialogue, advise through in-house research, inspire new ideas and connect experts to develop sustainable solutions to build a more peaceful future.

The GCSP Policy Briefs Series

The GCSP Policy Briefs series addresses current security issues, deduces policy implications and proposes policy recommendations. It aims to directly inform policy- and decision-making of states, international organisations and the private sector.

Under the leadership of Ambassador Thomas Greminger, Executive Director of the GCSP, the series is edited by Professor Nayef Al-Rodhan, Director of the Geopolitics and Global Futures Department, and Doctor Tobias Vestner, Director of the Research and Policy Advice Department & Head of Security and Law, and managed by Ms Christine Garnier Simon, Administration and Coordination Manager, GCSP Geopolitics and Global Futures.

Geneva Centre for Security Policy
Maison de la paix
Chemin Eugène-Rigot 2D
P.O. Box 1295
1211 Geneva 1
Switzerland
Tel: + 41 22 730 96 00
Contact: www.gcsp.ch/contact
www.gcsp.ch

ISBN: 978-2-88947-450-9

About the author

Dr Gazmend Huskaj is an executive leader with a proven record of translating strategy into action, including leading security information coordination for the United Nations and directing intelligence on cyber-related issues for the Swedish Armed Forces. He currently heads the Global Cyber and Security Policy Programme at the Geneva Centre for Security Policy (GCSP), which advances international cooperation through executive education, diplomatic dialogue, and policy research.

He holds MSc degrees in Security and Risk Management (University of Leicester) and Information Security (Stockholm University). He is a Certified Information Security Manager (CISM) and an alumnus of executive programmes at the Harvard Kennedy School and the GCSP's European Training Course in Security Policy. He has also completed advanced studies at Cranfield University, the University of St Andrews and the KTH Royal Institute of Technology. His doctoral research focused on offensive cyberspace operations, and he is widely recognised for his work on their implications for international security policy.

Acknowledgements

I would like to express my sincere gratitude to Dr Lars Nicander, Senior Adviser at the Swedish Psychological Defence Agency, and Col Dr Josef Schröfl, Strategic Adviser to the Secretary General at the Austrian Ministry of Defence, for their insightful reviews and valuable comments on this policy brief.

Additionally, in accordance with *Nature*'s editorial guidance on the transparent use of large language models,[1] this article benefitted from the use of ChatGPT-5 (OpenAI) as a research and editorial assistant. The tool was employed to refine English grammar, enhance stylistic clarity and improve paragraph structure. All substantive analysis, interpretation and final responsibility for the content remain solely with the author.

[1] *Nature*, "Tools Such as ChatGPT Threaten Transparent Science; Here Are Our Ground Rules for Their Use", editorial, Vol.613(7495), doi: https://doi.org/10.1038/d41586-023-00191-1.

Introduction

Over the past decade, offensive cyberspace operations have expanded rapidly and reshaped international security. Once limited to a few major powers, currently dozens of states and some non-state actors possess these capabilities, reflecting the normalisation of cyberspace offensive capacity across the international system. This diffusion erodes the boundary between peace and conflict and complicates deterrence by introducing ambiguity, shortened decision cycles, and a higher risk of miscalculation.

At a time of increasing geopolitical competition, understanding how to manage the global spread of offensive cyberspace capabilities is vital to sustaining strategic stability and preventing the escalation of cyberspace-related crises. This policy brief therefore asks *how states can reduce the risks of miscalculation and escalation while preserving stability and international norms in cyberspace*. It argues that stability can be strengthened through greater transparency, stronger legal and normative frameworks, and practical multistakeholder cooperation. The brief proceeds by tracing the diffusion of offensive cyberspace operations, analysing escalation dynamics, examining policy and legal gaps, and concluding with recommendations for global cooperation.

The global rise of offensive cyberspace operations

By 2019, at least 40 states were able to mount cyberattacks, which is a four-fold increase since 2011.[2] This diffusion reaches far beyond the original cyber "majors", and is propelled by national interests that range from deterrence and defence to coercion, espionage, and political signalling.[3]

The barrier to entry is lower than in the kinetic domain, meaning that the diffusion of offensive cyberspace operations has in effect levelled the playing field. States such as Iran or North Korea – and even well-organised ransomware groups – can contest or potentially disrupt the activities and systems of great powers with effects disproportionate to their traditional means. For instance, North Korea's 2017 WannaCry ransomware attack paralysed health care and transport systems across Europe, while Iran's 2022 cyberattacks on Albanian government networks caused the Albanian government to temporarily suspend diplomatic relations with Iran.

Similarly, the 2021 SolarWinds supply-chain intrusion, which was attributed to a relatively small group in Russia's intelligence ecosystem, inflicted strategic costs on the United States without kinetic engagement. These examples underscore how cyberspace allows actors with modest conventional capacity to project influence across borders and challenge established hierarchies. The proliferation of such operations raises broader questions about their systemic effects on international security.

To examine how this diffusion manifests in practice, it is useful to consider how major powers have incorporated offensive cyber capabilities into their strategic doctrines. China exemplifies the shift: its doctrine now embeds offensive cyberspace operations as a pillar of its grand strategy, elevating cyberspace to a core arena of major-power rivalry.[4] The combination of empowered weaker actors and major-power investment has turned cyberspace into an intensely competitive and contested environment. In this environment, offensive capability is increasingly viewed as an indispensable lever of statecraft. This evolution is not confined to individual states: it also extends to collective security institutions seeking to adapt their doctrines and structures.

---

[2] J. Healey and R. Jervis, "The Escalation Inversion and Other Oddities of Situational Cyber Stability", *Texas National Security Review,* Vol.3(4), Fall 2020, pp.30-53, https://dx.doi.org/10.26153/tsw/10962; B.A. Hamzah, "Asean Must Do More to Combat Military Activities in Cyberspace", draft for discussion, https://sscthailand.org/assets/sscprogram/upload/present/session4/01%20Malaysia%20(NDUM)%20(paper).pdf.

[3] G. Huskaj et al., *Staters Uttalade Normer i Cyberrymden*, Stockholm, Försvarshögskolan, 2021, https://urn.kb.se/resolve?urn=urn:nbn:se:fhs:diva-10206; Council on Foreign Relations, "Cyber operations Tracker", 2025, https://www.cfr.org/cyber-operations/.

[4] T. Jiang, "China's Offensive Cyber Strategy and Its Implications for Global Cyber Stability", *Journal of Chinese Political Science*, Vol.28, 2023, pp. 127-149, https://doi.org/10.1007/s11366-022-09813-3.

NATO's post-2016 reforms exemplify the diffusion of offensive cyber power. After the Warsaw Summit recognised cyberspace as an operational domain, in 2017 the alliance created a Cyberspace Operations Centre (COC) at Supreme Headquarters Allied Powers Europe. The COC reached initial operational capability in 2023, and is designed to deliver round-the-clock situational awareness[5] in a way that resembles the US "persistent engagement" operational framework.

The 2018 NATO Brussels Summit then authorised commanders to employ "sovereign cyber effects, provided voluntarily by Allies",[6] thereby starting to operationalise a collective analogue of the US "defend forward" doctrine, a proactive approach aimed at detecting and countering hostile cyber activity at its source rather than waiting for it to reach national networks. This doctrine forms part of the broader operational philosophy of persistent engagement, which emphasises continuous interaction with adversaries to shape their behaviour and impose costs through sustained contact. The overall objective was to enable action before threats could reach NATO systems.[7]

Major NATO members have established dedicated units that are capable of both defensive and offensive operations, such as the United Kingdom's National Cyber Force[8] and Germany's Cyber and Information Domain Service.[9] Yet decision thresholds and legal authorities remain opaque, while competition for exploitable zero-day vulnerabilities (i.e. previously unknown software flaws that attackers could use before developers instal patches) could potentially lead to arms-race-like behaviour. Smaller NATO allies can therefore realign doctrine and invest in scalable offensive capacity via, for example, public-private malware-engineering partnerships,[10] although such developments are guided more by alliance-level norms and voluntary contributions than by formal standardisation agreements.

Among the principal cyber powers, Russia couples disruptive malware, such as the NotPetya operation that spread far beyond its initial targets, with hack-and-leak campaigns in which stolen data is strategically released to influence political processes. These activities are often coordinated with conventional attacks to preserve strategic ambiguity. China, by contrast, conducts large-scale cyber intelligence collection targeting commercial and defence sectors,

[5] NATO (North Atlantic Treaty Organization), "Cyber Defence", 2024, https://www.nato.int/cps/en/natohq/topics_78170.htm.

[6] NATO CCDCOE (Cooperative Cyber Defence Centre of Excellence), "Cyber Defence at the 28th NATO Summit in Brussels, 11-12 July 2018", https://ccdcoe.org/incyder-articles/cyber-defence-at-the-28th-nato-summit-in-brussels-11-12-july-2018/.

[7] Ibid.

[8] UK Government, "National Cyber Force", 2024, https://www.gov.uk/government/organisations/national-cyber-force/about.

[9] Bundeswehr, "The Cyber and Information Domain Service", 2020, https://www.bundeswehr.de/en/organization/the-cyber-and-information-domain-service.

[10] J. Skingsley, "Offensive Cyber Operations: States' Perceptions of Their Utility and Risks", Royal Institute of International Affairs, 19 September 2023, https://doi.org/10.55317/9781784135850.

integrating cyber intelligence, surveillance, and reconnaissance into broader power-projection goals.[11]

Both Russia and China increasingly signal that cyber means can deliver coercive leverage while remaining below the threshold of an "armed attack" under Article 51 of the UN Charter, the clause that recognises a state's inherent right to self-defence, thereby complicating classical deterrence calculus. Espionage through cyberspace is a long-standing practice among all technologically advanced states and, just like traditional espionage, is not regulated in international law. Beyond these principal actors, a growing number of middle-tier states are emulating similar patterns, adapting offensive capabilities to their own regional contexts.

Middle-tier actors mirror this trajectory. Iran employs offensive cyberspace operations to offset its conventional shortfalls by putting Gulf energy infrastructure at risk; India's 2018 Defence Cyber Agency signals an outward-looking posture intended to reinforce deterrence beyond its immediate neighbourhood; and North Korea, despite severe resource constraints, has demonstrated global reach through ransomware and politically charged intrusions.[12]

Research by Khoirunnisa et al. seems to reaffirm a pattern: states such as China, Iran, Israel, and North Korea – and allegedly also the United States in the context of the Stuxnet operation – increasingly weave offensive cyber options into doctrines that once privileged defence. This trend contributes to what appears to be a diffusion and normalisation of such practices.[13] Comparative surveys of national cybersecurity strategies similarly highlight how governments often borrow phrasing and structural choices from perceived leaders such as the United States, United Kingdom, Australia, and Singapore.

France, for instance, set an early tone by stating in its 2011 national strategy an ambition to be a "cyberdefence world power" and join the "inner circle of major nations",[14] a goal similar to those later echoed in China's strategy. Germany publicly confirmed in 2012 that it had offensive cyber capabilities, but provided

[11] D. Mussington, "Strategic Stability, Cyber Operations and International Security", Centre for International Governance Innovation, 2019, https://www.cigionline.org/articles/strategic-stability-cyber-operations-and-international-security/; NATO CCDCOE, *Cyberspace Strategic Outlook 2030: Horizon Scanning and Analysis*, Tallinn, NATO CCDCOE Publications, 2022.

[12] IISS (International Institute for Strategic Studies), "Cyber Capabilities and National Power: India", 2021, https://www.iiss.org/globalassets/media-library---content--migration/files/research-papers/cyber-power-report/cyber-capabilities-and-national-power---india.pdf; Institute of South Asian Studies, "Going on the Offensive: India's Cyber Capabilities", National University of Singapore, 2020, https://www.isas.nus.edu.sg/papers/going-on-the-offensive-indias-cyber-capabilities/; S. Kiran, "A Comprehensive Study of India and Pakistan's Cyber Strengths and Weaknesses", Modern Diplomacy, 15 May 2023, https://moderndiplomacy.eu/2023/05/15/a-comprehensive-study-of-india-and-pakistans-cyber-strengths-and-weaknesses/; SGDSN (Secrétariat Général de la Défense et de la Sécurité Nationale), "Information Systems Defence and Security: France's Strategy", Paris, 2011, p.3; IISS, *Cyber Capabilities and National Power Volume 2*, 2023, https://www.iiss.org/research-paper/2023/09/cyber-capabilities-national-power-volume-2/.

[13] K. Khoirunnisa et al., "Comparative Analysis of National Cyber Defense Strategies: Implications for OCO Proliferation", *China Quarterly of International Strategic Studies*, 2025, https://doi.org/10.1142/S2377740025500010.

[14] SGDSN, 2011.

no information about their use.[15] This tendency toward "copy-pasting" policy concepts suggests a broader diffusion of doctrinal language, with echoes of forward-leaning operational postures such as "persistent engagement" and "defend forward" shaping the strategic lexicon.[16] The growing acceptance of deception-based and pre-emptive operations further blurs traditional escalation ladders and complicates strategic signalling.

In Southeast Asia, emergent military cyber units and tentative regional coordination have produced an offence-dominant security dilemma that deepens mistrust and raises the prospect of the inadvertent escalation of cyberspace-related crises.[17]

The Council on Foreign Relations' Cyber Operations Tracker indicates a steady rise in incidents across all regions, spanning espionage, sabotage, data destruction and politically motivated disruptions.[18] This pattern underscores the importance of dialogue and transparency as the means to reduce the risk of crisis escalation.

Risks of miscalculation and escalation

Offensive cyberspace operations fuse anonymity, compressed decision timelines, and blurred thresholds for what may constitute the use of force or an armed attack. These features may increase the risk of miscalculation and escalation, since deterrence in cyberspace, though not unique in its reliance on perceptions and uncertainty, is harder to operationalise when attribution is contested and "red lines" are rarely declared.[19]

According to recent research, most state activity occurs in what is known as the "grey zone" – a spectrum of competition between peace and war where coercive actions remain intentionally ambiguous and below the threshold of an "armed attack" under Article 51 of the UN Charter. This would allow state and non-state actors to conduct intrusions, disinformation, and low-level disruption without triggering formal defence commitments.[20] While escalation spirals remain rare to date, repeated low-grade actions can potentially create

[15] IISS, 2023.

[16] F. Heiding et al., "Cybersecurity Strategy Scorecard", Belfer Center for Science and International Affairs, Harvard Kennedy School, https://www.belfercenter.org/research-analysis/cybersecurity-strategy-scorecard.

[17] Hamzah, 2019; M. Richey, "Cyber Offence Dominance, Regional Dynamics, and Middle Power-led International Cooperation", in G. Boulet et al. (eds), *Cybersecurity Policy in the EU and South Korea from Consultation to Action: Theoretical and Comparative Perspectives*, Cham, Palgrave Macmillan, 2022, pp.67-97, https://doi.org/10.1007/978-3-031-08384-6_4.

[18] Council on Foreign Relations, "Cyber Operations Tracker", 2025, https://www.cfr.org/cyber-operations/.

[19] G. Huskaj, "Offensive Cyberspace Operations: Implications for Sweden", PhD thesis, Department of Computer and Systems Sciences, Stockholm University, 2024.

[20] P. Pernik (ed.), *Cyberspace Strategic Outlook 2030: Horizon Scanning and Analysis*, NATO CCDCOE, 2021, https://ccdcoe.org/library/publications/cyberspace-strategic-outlook-2030-horizon-scanning-and-analysis/.

tit-for-tat exchanges that under certain conditions may spiral out of control and erode strategic stability.[21]

Attribution uncertainty may complicate state response: obfuscation, proxies, and jurisdiction-hopping can misdirect retaliation and weaken deterrence.[22] Although escalation from misattribution is uncommon, compressed timelines in crises may pressure leaders to act prematurely, risking occasional, but serious, confrontations.[23]

The 2010 Stuxnet incident underscores the risks inherent in covert cyberspace operations: its initially ambiguous attribution[24] and unintended global spread fuelled fears of escalation[25] and prompted many states to accelerate their development of offensive cyber doctrines and capabilities. Subsequent forensic work revealed that the operation had a narrowly defined objective: to disrupt Iran's uranium-enrichment centrifuges. The incident showed that when cyberspace operations are kept secret, other states can easily misunderstand their purpose. Such misunderstandings can fuel competition, especially when military doctrine interprets the surreptitious placement of code inside networks as preparation for future attacks.

While these cases highlight how opacity can potentially heighten escalation, Jiang's[26] research on China's evolving cyber doctrine suggests that limited signalling and occasional restraint mechanisms can temper escalation risks, even as technical capacity expands – although, as Jiang notes, opacity continues to dominate.[27]

Although, according to Jiang, some restraint exists, opacity and the absence of universally accepted definitions of a cyberattack or use of force mean that every actor interprets intent and legality through its own strategic lens. Deep civilian-military interdependence ensures that large-scale intrusions likely jeopardise public welfare far beyond military targets. NATO assessments note that militaries increasingly rely on civilian-run networks such as logistics, energy, and communications, where vulnerabilities migrate easily across domains. As a result, cyberattacks intended for military command-and-control systems can cascade into disruptions of hospital, transport or financial systems, underscoring the inseparability of societal resilience from military readiness.[28]

---

[21] Hamzah, 2019.

[22] S. Baliga et al., "Deterrence with Imperfect Attribution", *American Political Science Review*, Vol.114(4), 2020, pp.1155-1178.

[23] Healey and Jervis, 2020.

[24] Huskaj, 2024.

[25] J.R. Lindsay, "Stuxnet and the Limits of Cyber Warfare", *Security Studies*, Vol.22(3), 2013, pp.365-404, https://doi.org/10.1080/09636412.2013.816122.

[26] T. Jiang, "The Shift of China's Strategic Thinking on Cyberwarfare Since the 1990s", *Journal of Chinese Political Science*, Vol.28, 2023, https://doi.org/10.1007/s11366-022-09813-3.

[27] Ibid.

[28] Pernik (ed.), 2021; Huskaj, 2024

These global challenges also appear in regional settings. Comparative work on Latin America indicates that weak legislative oversight and opaque intelligence authorities can elevate the risk of escalation, especially when offensive cyber units lack civilian control, leading scholars to recommend capacity-building activities and the implementation of confidence-building measures (CBMs) focused on rapid communication and clearer legal frameworks.[29]

In sum, offensive cyberspace operations can act as systemic risk amplifiers when left unconstrained. Ambiguity and the slow development of shared norms leave cyberspace vulnerable to inadvertent confrontations. Mitigating this danger demands pragmatic confidence-building, hotlines, incident notification, and renewed dialogue aimed at transparency and reciprocal restraint.[30] Yet even as these operational risks are increasingly recognised, the legal and policy frameworks meant to govern state behaviour in cyberspace have not kept pace.

Policy blind spots and legal ambiguity

The diffusion of offensive cyberspace operations has outpaced legal and policy development, amplifying strategic ambiguity. Strategic silence pervades the domain, because most states rarely declare response thresholds or publicly acknowledge their offensive capabilities. A handful of states, particularly several Five Eyes members,[31] have begun limited public disclosures of their offensive capabilities, but uncertainty remains. In the absence of declared "red lines", states may interpret boundaries differently, and although uncommon, operations intended as espionage could be perceived as preparatory steps toward escalation.[32]

The international legal architecture is poorly adapted to the cyber context. Existing law, rooted in the UN Charter and the traditional law of armed conflict, struggles to accommodate offensive cyberspace operations and cyberspace as a whole. Many operations fall below the "armed attack" threshold, involving disruption or data theft rather than physical aggression. This has created a persistent legal grey zone. In this vacuum, states like Russia push the limits of hybrid warfare and exploit their adversaries' hesitation over whether a particular act warrants a forceful response.[33] Various types of critical infrastructure,

[29] D. Álvarez-Valenzuela and F. Vera-Hott, "Cyber Operations in South America", *Baltic Yearbook of International Law*, Vol.20, 2022, pp.163-186; Richey, 2022.

[30] E.D. Borghard and S.W. Lonergan, "Confidence Building Measures for the Cyber Domain", *Strategic Studies Quarterly*, Vol.12(3), 2018, https://www.airuniversity.af.edu/Portals/10/SSQ/documents/Volume-12_Issue-3/Borghard-Lonergan.pdf; Huskaj, 2024.

[31] Australia, Canada, New Zealand, United Kingdom, and United States; see Pernik (ed.), 2021.

[32] Just Security, "Cyber Espionage", 2025, webpage, https://www.justsecurity.org/tag/cyber-espionage/.

[33] Pernik (ed.), 2021.

ranging from hospitals to satellite services, share the same networks, so even a narrowly targeted activity can lead to civilian harm.[34]

Attempts to clarify responsible behaviour have produced limited, non-binding outcomes. The UN Group of Governmental Experts and the Open-Ended Working Group (OEWG) have issued voluntary norms, yet major-power rivalry and divergent priorities block a binding treaty. Consequently, debate has split between those urging the full implementation of existing norms and those demanding new legal rules, leaving a patchwork of doctrines without universal enforcement.[35] Regional bodies such as the Organization for Security and Co-operation in Europe (OSCE) and the Association of Southeast Asian Nations (ASEAN) pilot CBMs, but while the OSCE enjoys near-universal uptake among its members, participation and mandate remain uneven across ASEAN and other regions.

Attribution and accountability form further blind spots. Although the attribution of major attacks to specific perpetrators is increasingly common, no international forum adjudicates state responsibility or applies sanctions. Where naming and shaming fail, retaliatory measures remain ad hoc. One proposal gaining traction among middle powers is a UN-based cyber incidents arbitration panel, but it remains at the concept stage, awaiting broad political buy-in before it could adjudicate responsibility and assign remedies.[36]

The absence of legal clarity is a structural vulnerability. States operate without a shared understanding of the concepts of aggression, thresholds, or accountability, and comparative studies show that these gaps both stem from and feed strategic mistrust, depriving the international community of reliable mechanisms for crisis management.[37] Converging on the "rules of the road", clarifying attribution procedures, and strengthening CBMs therefore remain essential for reducing instability and preventing future crises. Building on these gaps, the next logical step involves ascertaining how states can move from identifying vulnerabilities to fostering responsible conduct that mitigates them.

Toward responsible state behaviour

The accelerating diffusion of offensive cyberspace operations makes fostering responsible state behaviour an urgent imperative for strategic stability and risk reduction. As the international community grapples with persistent ambiguity, the absence of clear thresholds, and the risk of rapid escalation, pragmatic CBMs,

[34] A. Carlo et al., "The Challenge of Protecting Space-Based Assets against Cyber Threats", *Proceedings of the International Astronautical Congress*, 2020, pp.1-8.

[35] Hamzah, 2019.

[36] Mussington, 2019.

[37] Richey, 2022.

enhanced dialogue, and capacity-building measures emerge as indispensable elements of cooperative security.[38]

Recent multilateral discussions, such as the OEWG's tenth substantive session, underscored that cyber threats are transnational and demand collective rather than unilateral responses. Delegations stressed cooperative measures such as capacity-building, knowledge sharing and incident management as essential to reducing risks.[39] Complementing this, scholarship highlights the importance of whole-of-society approaches, including regional knowledge transfer, public-private partnerships and engagement with technical communities, as key to building resilient cyber security capacity.[40]

Applying these principles in practice, concrete steps toward responsible state behaviour include the operationalisation of CBMs such as the notification of major cyber incidents, the establishment of cyber "hotlines" and joint crisis management exercises, which can act as critical off-ramps during periods of heightened tension.[41] The development of points of contact (POC) directories encompassing diplomatic, technical, and operational representatives facilitates rapid communication and clarifies intent. Yet the tenth OEWG session described CBM implementation as "subdued", with inconsistent activation of the 116-state POC directory.[42] Thus, the uneven implementation of POC mechanisms and inconsistent thresholds for information exchange highlight the need for clearer guidance and regular scenario-based exercises to test and refine procedures.

Military-to-military dialogue must adapt to the realities of cyberspace, leveraging trusted communication channels to support mutual understanding, deconfliction and the clarification of intentions, particularly during periods of crisis.[43] Regional organisations, including the OSCE, ASEAN, and the African Union (AU), can serve as conveners of Track 1.5 and Track 2 dialogues, allowing strategic competitors to share best practices, signal restraint, and build habits of cooperation. These multilateral settings are critical for the exchange of lessons learned, the articulation of emerging threats and the promotion of cyber resilience.[44]

Moreover, international efforts to embed norms of responsible state behaviour through voluntary non-binding agreements, or, eventually, formal treaties can reinforce mutual expectations, clarify permissible conduct, and reduce ambiguity

[38] Mussington, 2019.

[39] Digital Watch Observatory, "OEWG's Tenth Substantive Session: Entering the Eleventh Hour", 27 February 2025, https://dig.watch/updates/oewgs-tenth-substantive-session-entering-the-eleventh-hour.

[40] G. Huskaj and S. Axelsson, "A Whole-of-Society Approach to Organise for Offensive Cyberspace Operations: The Case of the Smart State Sweden", *Proceedings of the 22nd European Conference on Cyber Warfare and Security*, Vol.22, 2023, pp.592-601.

[41] Hamzah, 2019.

[42] Digital Watch Observatory, 2025.

[43] Borghard and Lonergan, 2018.

[44] Ibid.

in cyberspace operations.[45] While consensus on binding legal mechanisms remains vague, incremental progress in voluntary norm development and CBM implementation is essential for reducing miscalculation and supporting cooperative crisis management.[46] Ultimately, it is the institutionalisation of dialogue, regular information exchange, and reciprocal restraint that will enable states to mitigate the risks posed by offensive cyberspace operations and sustain a more stable and predictable international cyber environment. Translating these principles into concrete action requires mechanisms for global cooperation that can bridge political divides and operationalise shared norms.

Recommendations for global cooperation

Effective global cooperation remains indispensable for mitigating the risks that accompany the widening diffusion of offensive cyberspace operations. No single state, sector or region can shoulder the complexity of cross-border cyber threats; collective security therefore demands coordinated, multistakeholder responses linking governments, industry, academia and civil society. Institutions with Track 1.5 convening capacity that are able to bridge official and non-official channels are well placed to translate policy recommendations into practical solutions. They are able to do so by hosting dialogue activities on topics of interest for convened practitioners, who can then carry insights gained back into national policy processes.

Firstly, cooperation should be anchored in harmonised legal frameworks and clear operational norms. At the OEWG's tenth substantive session, delegations emphasised capacity-building and knowledge sharing as central to managing cyber threats, while debates continued over whether to prioritise the implementation of agreed norms or the development of new ones. Progress on legal convergence remained limited, underscoring the challenge of translating voluntary commitments into concrete, implementable standards.

Secondly, regional organisations can act as arenas for cooperation. The OSCE, ASEAN, and AU already help their members exchange best practices, pilot CBMs, and cultivate habits of cooperation even among strategic competitors. For example, the OSCE established a cyber POC directory in 2016 to improve incident communication, while ASEAN has piloted joint cyber capacity-building exercises under its Defence Ministers' Meeting-Plus framework.

Their practical projects range from joint crisis simulations to shared, standardised incident-notification templates transmitted in common data formats such as STIX and TAXII (Structured Threat Information Expression/Trusted Automated Exchange of Indicator Information). These open technical standards enable the automated and machine-readable exchange of cyber-threat data between organisations' cybersecurity systems, improving situational awareness and

[45] Ibid.

[46] Richey, 2022.

coordination when such systems are available. This demonstrates how modest, region-specific steps can lower escalation risks and strengthen collective awareness. Facilitating regional dialogue, designing pilots and ensuring lessons learned are shared across regions will be critical.

Thirdly, Track 1.5 diplomacy (semi-official dialogue that brings together government officials and independent experts) remains a vital bridge between formal negotiations and informal expert engagement. When treaty talks stall, roundtables and scenario exercises that combine diplomatic, technical, and academic perspectives can help identify emerging risks, improve approaches to advance notification, and build trust. Extending these platforms to underserved regions will ensure that insights feed back into official forums and crisis-management channels alike.

Fourthly, cooperation that builds future capacity must invest in strong organisations and broad participation. Expanded training programmes and knowledge sharing among developing countries (South-South cooperation) can increase the number of practitioners able to put cyber norms and incident-response procedures into practice in diverse contexts. Executive courses and practitioner networks linking emerging and established cyber powers should include diverse perspectives to ensure that policy solutions are globally relevant.

Fifthly, putting voluntary norms into practice requires clear decision-making processes, regular information exchange and CBMs that can be monitored. Comparing national approaches can highlight implementation gaps and support the co-design of new CBMs suited to emerging technologies such as quantum-resistant encryption and AI-enabled intrusion detection.

Finally, cooperation must remain flexible enough to adjust quickly to new threats. Small working groups and temporary coalitions can bring governments and non-state actors together to address emerging risks and rapid technological changes. Holding short-notice meetings, commissioning studies on future risks and testing policy ideas in practice before they reach formal negotiations will help to keep progress on track.

In short, the best way to prevent offensive cyberspace operations from creating instability is to follow a strategy built on shared understanding and cooperation. This includes clearer agreement on how international law and voluntary norms apply, the development of regional pilot projects, regular Track 1.5 dialogue, broad capacity-building across sectors, and the timely adoption of agreed practices. Together, these measures can help build a cooperative and stable international cyber environment.

Building Peace Together

Geneva Centre for Security Policy
Maison de la paix
Chemin Eugène-Rigot 2D
P.O. Box 1295
1211 Geneva 1
Switzerland
Tel: + 41 22 730 96 00
Contact: www.gcsp.ch/contact
www.gcsp.ch

ISBN: 978-2-88947-450-9

GCSP
Geneva Centre for Security Policy