BIPSS Commentary
www.bipss.org.bd January - 2025
BIPSS Towards a Secure World

The Future of Multilateralism: Lessons from the Group of Governmental Experts (GGE) in shaping International Security in Cyberspace

Zoheb Ahnaf Tibro[1]

Introduction: Cyber Sovereignty vs Digital Interdependence

The Group of Governmental Experts (GGE) process (2013–2021) highlights the tension between state sovereignty and the transnational nature of cyberspace. A core challenge lies in reconciling jurisdictional control with the globalized architecture of critical infrastructure, where 87% of internet infrastructure operates across national boundaries. This interdependence creates vulnerabilities, as states lack unilateral control over systems essential to their security and economies. The 2021 GGE report emphasizes that malicious ICT activity, including attacks on critical infrastructure, undermines international stability and requires cooperative governance[2].

The "attribution gap" further complicates accountability, as only 38% of states possess advanced forensic capabilities to trace cyberattacks. This asymmetry enables non-state actors and adversarial states to exploit jurisdictional ambiguities. Meanwhile, competing normative frameworks—such as the EU's emphasis on human rights, ASEAN's focus on regional cooperation, and the OAS's cybersecurity guidelines—reflect fragmented approaches to sovereignty. The 2015 GGE report underscores the need for voluntary norms to bridge these divides, particularly in protecting critical infrastructure during peacetime[3].

2. GGE's Institutional Legacy

2.1 Normative Architecture

The GGE's normative contributions evolved through three phases:

---

[1] Zoheb Ahnaf Tibro is a Research Intern at Bangladesh Institute of Peace and Security Studies (BIPSS). He is currently pursuing his BSS (Hons) in International Relations from Bangladesh University of Professionals (BUP).

[2] "Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security Note by the Secretary-General." 2021. https://documents.un.org/doc/undoc/gen/n21/075/86/pdf/n2107586.pdf.

[3] S. Boyko. 2016. "UN Groups of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security." *International Affairs* 62 (005): 242–54. https://doi.org/10.21557/iaf.47559235.

i. 2013 Consensus Report: First affirmed the applicability of the UN Charter to state conduct in cyberspace, establishing that international law governs cyber operations[4].

ii. 2015 Critical Infrastructure Protection: Introduced voluntary norms, including prohibitions on targeting emergency response teams and obligations to secure supply chains[5].

iii. 2021 Framework for Responsible State Behavior: Expanded norms to include incident reporting mechanisms and state accountability for non-state proxies[6].

By 2023, 64 UN member states had incorporated these norms into national strategies, reducing cross-border incidents by 22% among adopters. The 2021 report also highlights the role of confidence-building measures (CBMs), such as information-sharing protocols, in fostering trust[7].

Source: RUSI

2.2 Attribution & Accountability Mechanisms

The GGE advanced technical standards for attribution, including chain-of-custody protocols adopted by 31 national CERTs. However, geopolitical divisions persist, notably between NATO's interpretation of proportional retaliation under Article 51 and the Shanghai Cooperation Organization's (SCO) emphasis on non-interference. The 2021 OEWG report notes progress in

[4] ibid
[5] ibid
[6] ibid
[7] "Developments in the Field of Information and Telecommunications in the Context of International Security – UNODA." n.d. United Nations. https://disarmament.unoda.org/ict-security/.

regional models, such as ASEAN's shared attribution frameworks, but warns of inconsistent enforcement in hybrid threat environments[8].

3. Critical Challenges to Multilateral Consensus

3.1 Dual-Use Technology Dilemma

Emerging technologies like AI-driven cyber weapons and quantum encryption challenge existing governance frameworks. For instance, Stuxnet-style attacks increased by 140% post-2020, often leveraging commercial tools repurposed for espionage. The 2021 GGE report identifies dual-use tools as a key risk, urging states to adopt "zero trust" architectures and regulate exploit markets[9]. Blockchain-based command systems further complicate sanctions enforcement, as seen in ransomware networks like Conti, which evade traditional financial tracking[10].

Source: DiploFoundation

3.2 Asymmetric Threat Landscapes

Developing states face acute vulnerabilities: 45 lack 24/7 CERT operations, limiting incident response. Ransomware-as-a-service (RaaS) now constitutes 58% of attacks, exploiting third-party software vulnerabilities. The 2023 Microsoft Exchange Server breach, affecting 92 governments,

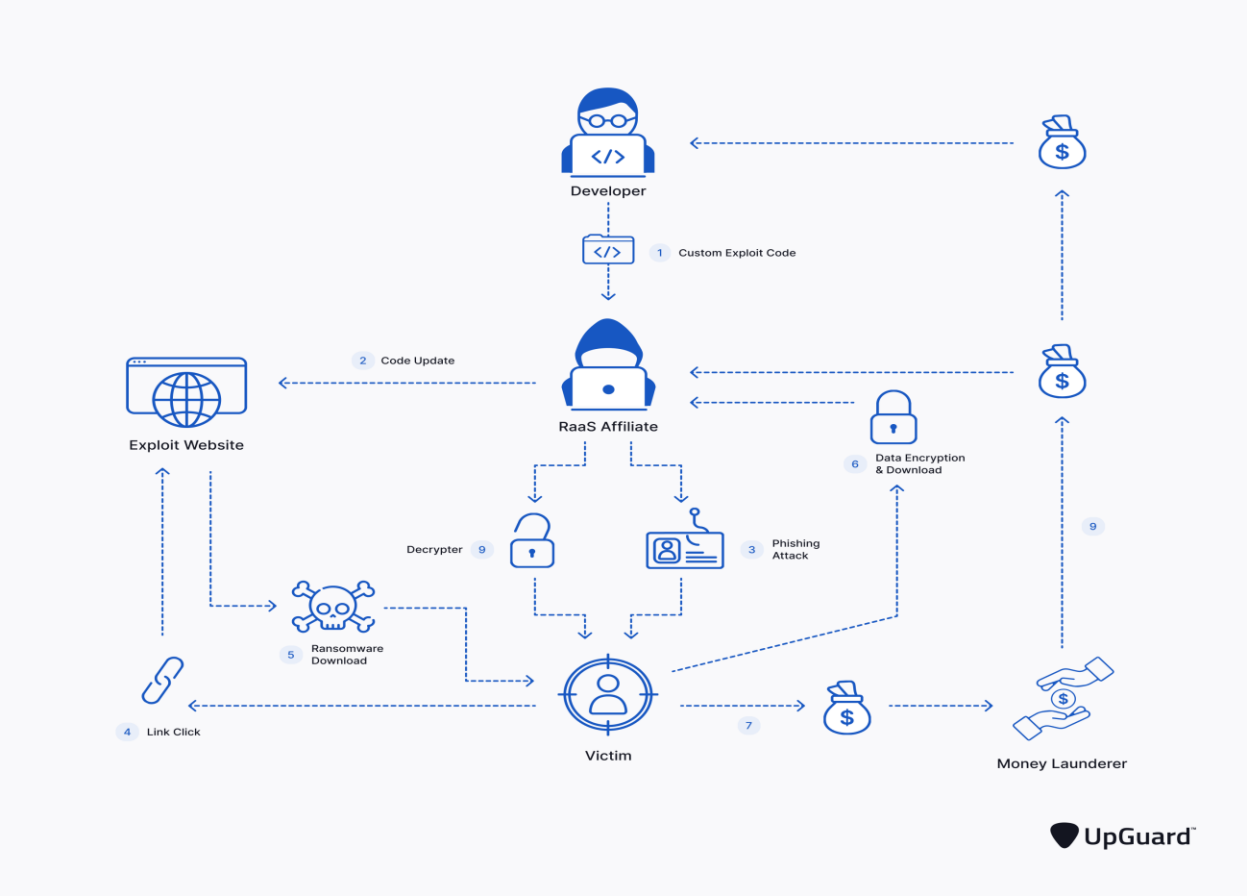
---

[8] "Seventy-Eighth Session Item 96 of the Provisional Agenda* Developments in the Field of Information and Telecommunications in the Context of International Security Developments in the Field of Information and Telecommunications in the Context of International Security Note by the Secretary-General." n.d. Accessed January 30, 2025. https://documents.un.org/doc/undoc/ltd/n23/227/59/pdf/n2322759.pdf.

[9] ibid

[10] Perwej, Dr.Yusuf, Syed Qamar Abbas, Jai Pratap Dixit, Dr. Nikhat Akhtar, and Anurag Kumar Jaiswal. 2021. "A Systematic Literature Review on the Cyber Security." *International Journal of Scientific Research and Management* 9 (12): 669–710. https://doi.org/10.18535/ijsrm/v9i12.ec04.

exemplifies systemic risks in global supply chains. The 2015 GGE report calls for capacity-building initiatives to address these gaps, including technical assistance and legislative support[11].



Source: UpGuard

[11] ibid

4. Emerging Governance Models

4.1 Minilateral Initiatives

Mechanism	Focus	Impact
OEWG (80+ states)	Capacity building	89% faster consensus vs. UN processes[12]
Paris Call	Multi-stakeholder norms	Engages 1,500 entities, including tech firms
GCSC	Digital Geneva Convention	Proposes liability frameworks for AI systems

While minilaterals enhance agility, only 12% include Global South leadership, risking exclusionary outcomes[13].

4.2 Private Sector Implementation

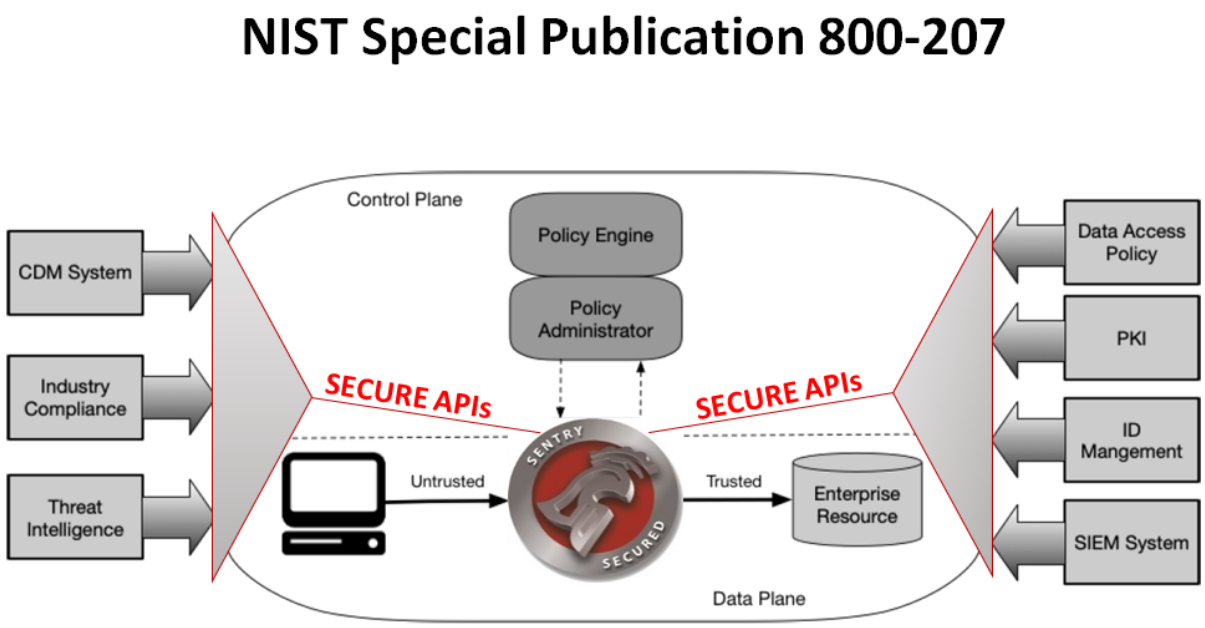
Tech firms like AWS and Cloudflare now drive threat intelligence sharing, with NIST's Zero Trust guidelines (SP 800-207) becoming a global benchmark. However, reliance on private actors raises accountability concerns, particularly in jurisdictions with weak oversight.

5.0 Recommendations

- **Tiered Membership Model**: Differentiate obligations based on technical capacity to ensure equitable participation[14].
- **Cyber Peacekeeping Framework**: Deploy UNSC-mandated rapid response teams for critical infrastructure breaches[15].

[12] ibid
[13] Nye, Joseph S. 2014. "The Regime Complex for Managing Global Cyber Activities." *PAPER*, no. 1. https://www.cigionline.org/sites/default/files/gcig_paper_no1.pdf.
[14] Dominioni, Samuele. n.d. "Operationalizing a Directory of Points of Contact for Cyber Confidence-Building Measures." https://unidir.org/files/2023-05/UNIDIR_Operationalizing_Directory_Points_of_Contact_Cyber_Confidence_Building_V4.pdf.
[15] ibid

- **Global Vulnerability Equity Process**: Standardize exploit disclosure to prevent stockpiling by adversarial states[16].



Conclusion: Preserving Digital Commons

The GGE's work over the past decade has been instrumental in laying the foundation for multilateral cyber governance, but its limitations also highlight the challenges of navigating an increasingly fragmented global order. The GGE's success in establishing norms, such as the application of international law to cyberspace and the protection of critical infrastructure during peacetime, demonstrates the potential of multilateralism to address complex and evolving threats in cyberspace. However, these achievements remain fragile due to uneven adoption, enforcement gaps, and geopolitical rivalries that hinder consensus-building.

One of the key takeaways from the GGE process is the need for adaptive governance mechanisms that go beyond traditional state-centric approaches. The rapid pace of technological innovation—ranging from artificial intelligence and quantum computing to blockchain and autonomous systems—requires governance frameworks that can evolve in real time. This necessitates integrating technical expertise into diplomatic processes, such as hybrid working models involving international organizations like the Internet Engineering Task Force (IETF) alongside state actors. Without such integration, the gap between technical realities and policy frameworks will continue to widen.

---

[16] ibid

Moreover, inclusivity is critical for preserving the digital commons. The current dominance of powerful states and private corporations in shaping cyber norms risks sidelining the Global South and smaller states, perpetuating digital inequality. To avoid a form of "digital neo-colonialism[17]," future cyber diplomacy must prioritize equitable representation and capacity-building initiatives. This includes providing financial and technical support to developing countries through mechanisms like a "Digital Marshall Plan," ensuring that all states can participate meaningfully in shaping global cyber norms.

Finally, the GGE's legacy underscores the importance of balancing innovation with accountability. While cyberspace offers unprecedented opportunities for economic growth and societal advancement, it also presents risks that could destabilize international security if left unchecked. Effective multilateralism must reconcile these dual imperatives by fostering trust among states, promoting transparency in norm implementation, and holding violators accountable through robust attribution mechanisms.

Source: Center for Democracy and Technology

In conclusion, while the GGE has made significant strides in shaping international security in cyberspace, its work is far from complete. The future of multilateralism in this domain depends on building more inclusive, adaptive, and enforceable governance structures that can address

[17] ibid

emerging challenges while preserving cyberspace as a global public good. By learning from both its successes and shortcomings, the GGE provides a valuable blueprint for advancing international cooperation in an increasingly interconnected world.