Scientific and Practical Cyber Security Journal (SPCSJ) 8(4): 91 – 94 ISSN 2587-4667 Scientific Cyber Security Association (SCSA)

APPLICATION OF INTERNATIONAL LAW IN CYBERSPACE

Joanna Kulesza, PhD
Assistant Professor, Department of Public International Law, University of Lodz Law School;
Executive Director, Lodz Cyber Hub, University of Lodz, Poland.

ABSTRACT: This paper examines the evolving role of international law in cyberspace, with a focus on the contributions of the United Nations through its Group of Governmental Experts (UN GGE) and Open-Ended Working Group (OEWG). It analyzes key principles affirmed by the UN GGE, such as sovereignty, non-intervention, and due diligence, while highlighting challenges stemming from limited participation and divergent state views. The paper also explores the OEWG's broader approach to inclusivity and its efforts to address unresolved issues. Furthermore, it assesses the 2024 European Declaration on the Application of International Law in Cyberspace, emphasizing its role in complementing UN initiatives and strengthening global cyber governance. By bridging theoretical frameworks with actionable measures, the paper underscores the importance of multilateral cooperation in addressing cyber threats and advancing a rules-based international order in the digital age.

KEYWORDS: international law, cybersecurity, Internet governance, human rights, due diligence.

INTERNATIONAL LAW IN CYBERSPACE: UN GGE, OEWG, AND THE EUROPEAN DECLARATION

The rapid evolution of cyberspace has posed significant challenges to the application of international law, requiring enhanced dialogue and collaboration among states and non-state actors. As the digital domain increasingly shapes global interactions, international institutions have become necessary to effectively address legal questions surrounding state behaviour in and governance of cyberspace. The establishment of norms and principles to govern this domain highlights the importance of balancing state sovereignty with collective security. In this context, the United Nations has played a vital role in advancing discussions on the applicability of international law to cyberspace, fostering multilateral cooperation, multistakeholder governance and addressing complex global issues of security, responsibility and human rights.

Among its numerous initiatives, two platforms have played a key role: the Group of Governmental Experts (UN GGE) and the Open-Ended Working Group (OEWG). The UN GGE, established in 2004, has made significant contributions, particularly through its 2013 and 2015 reports, which affirmed that existing international law, including the UN Charter, applies to cyberspace.[1] These reports also introduced foundational principles such as state sovereignty, non-intervention, and the peaceful settlement of disputes in the digital domain. However, the GGE's limited membership and difficulty achieving consensus have underscored challenges in addressing diverse state perspectives.

To overcome these limitations, the OEWG was established in 2018, offering a more inclusive platform for dialogue among all UN member states. Its broader participation aimed to address contentious issues left unresolved by the GGE, including interpretations of sovereignty and the principle of due diligence in cyberspace. Despite these efforts, divergent views among states persist, particularly concerning the extent of state responsibility for cyber operations and how international law should evolve to address emerging cyber threats.

The European Council Declaration on a Common Understanding of International Law in Cyberspace complements similar efforts of individual states and those of the UN by providing clarity and reinforcing

[1] See respectively: UN GGE 2013 Report: United Nations, Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, A/68/98 (24 June 2013). Available at: https://digitallibrary.un.org/record/752462; UN GGE 2015 Report: United Nations, Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, A/70/174 (22 July 2015). Available at: https://digitallibrary.un.org/record/799853 .

key legal principles in a vital geopolitical region.[2] Adopted in November 2024, the Declaration emphasizes state responsibility for cyber activities within their jurisdiction and highlights the applicability of sovereignty, non-intervention, and due diligence in cyberspace. By aligning with existing UN principles and frameworks, the Declaration strengthens the global legal regime governing state behaviour in cyberspace, addressing critical gaps and advancing collective understanding. It reflects Europe's commitment to fostering a rules-based international order while supporting ongoing multilateral discussions at the UN and complementary multistakeholder efforts in various Internet governance venues. Through its practical contributions, the Declaration bridges theoretical principles with actionable measures, setting a benchmark for responsible state behaviour in the digital age.

SHIFT TO INFRASTRUCTURES IN INTERNET GOVERNANCE AND RESPONSIBLE STATE BEHAVIOUR

The focus of internet governance has evolved significantly within the UN and in its members states since the adoption of the 2005 Tunis Agenda approved by the World Summit on the Information Society (WSIS), shifting from the establishment of normative frameworks toward the protection of critical infrastructures such as undersea cables and satellites. These infrastructures form the backbone of global connectivity, with undersea cables handling over 95% of international data traffic and satellites supporting a wide range of services, from communications to navigation. As cyberspace increasingly integrates terrestrial and orbital systems, the complexity of protecting this hybrid infrastructure grows, amplifying the need for effective governance and technical measures.

Under international law, states bear responsibilities to protect cyber infrastructure within their jurisdiction and ensure its resilience against attacks. These obligations stem from principles such as sovereignty and due diligence. Recent incidents, such as the severing of undersea cables disrupting internet access in regions like Northern Europe, and reports of satellite cyberattacks targeting communication networks, highlight the vulnerabilities of these systems. Such incidents not only compromise connectivity but also pose risks to national security, economic stability, and humanitarian operations.

Addressing these challenges requires collaboration across sectors and between various stakeholder groups. Public-private partnerships are particularly vital, as much of the critical infrastructure is owned and operated by private entities. The multistakeholder approach to Internet governance complements existing international law frameworks and brings together governments, corporations, technical experts, and civil society to ensure comprehensive policies and avoid fragmentation. These include setting technical standards for infrastructure security, implementing state policies that mandate protection, and fostering international agreements to manage shared vulnerabilities. Integrating these efforts into existing internet governance mechanisms strengthens the resilience of the digital ecosystem, emphasizing that securing infrastructure is as crucial as establishing norms. By prioritizing infrastructure security alongside legal frameworks, the international community can better safeguard the foundations of the interconnected world.

THE EUROPEAN DECLARATION ON INTERNATIONAL LAW IN CYBERSPACE

The recent European Declaration on a Common Understanding of International Law in Cyberspace, adopted by the Council of the European Union on November 18, 2024, represents a landmark for a shared regional understanding of legal norms for state behaviour in cyberspace. The Declaration draws heavily from established international frameworks, notably the International Law Commission's Articles on the Responsibility of States for Internationally Wrongful Acts (ARSIWA), reinforcing principles such as the attribution of wrongful acts and the conditions under which states may respond

[2] European Council, "Declaration on a Common Understanding of International Law in Cyberspace," Brussels, November 18, 2024, Document 15833/24, CYBER 334, COJUR 111, COPS 622.

to cyber operations. It stipulates that states are responsible for the actions of their organs and, under Articles 8 and 11 of ARSIWA, may also be held accountable for non-state actors acting under their instruction or whose actions they adopt as their own. The Declaration emphasizes discretion in whether to disclose attribution publicly or keep it confidential, balancing transparency and operational security.

In addressing responses to cyber incidents, the Declaration categorizes permissible actions into peaceful dispute resolution, retorsions, and measures under specific exceptions to wrongfulness, such as self-defense and countermeasures. Peaceful means remain paramount, aligning with Articles 2(3) and 33(1) of the UN Charter. At the same time, it recognizes retorsions, such as economic or diplomatic sanctions, as legitimate tools that do not breach international law. This nuanced framework reflects the EU's commitment to a stable, rules-based international order in cyberspace, linking existing legal principles to the realities of modern digital infrastructure.

By adopting this Declaration, the EU solidifies its role as a normative leader in cyberspace governance. It builds upon previous international consensus, such as the work of the UN GGE and the OEWG, while promoting practical guidance for state behaviour. Its implementation could enhance global cyber stability and set a model for broader international cooperation.

The European Declaration also underlines key principles of sovereignty, self-defence, and due diligence in cyberspace, affirming the need for state responsibility and liability. It explicitly addresses the responsibility of states for cyber operations originating within their jurisdiction, reinforcing that states must not allow their territories to be used for activities that breach international peace or security.

In terms of its impact on EU cyber diplomacy, the Declaration strengthens Europe's collective stance on cybersecurity and legal cooperation, fostering unified responses to cyber threats. It positions the EU as a leader in advocating for a rules-based international order in cyberspace, promoting collaboration between member states and external partners to enhance cybersecurity resilience. This approach strengthens law enforcement cooperation and shows the EU's commitment to a safe, stable, and accountable cyber environment.

CONCLUSIONS AND RECOMMENDATIONS

The evolving discourse on international law in cyberspace highlights its critical relevance in shaping responsible state behaviour and securing digital infrastructures. The European Declaration follows the path set by the UN GGE and the OEWG, numerous national positions on the application of international law in cyberspace, and the African Union one adopted earlier in 2024. It exemplifies a significant step toward harmonizing global perspectives. It reaffirms the applicability of established international law, emphasizing principles such as sovereignty, state responsibility, and due diligence, while promoting peaceful resolutions to disputes. Its alignment with multilateral frameworks and emphasis on practical state accountability strengthens the global cybersecurity architecture.

To ensure the effective implementation of these principles, several recommendations should be made. First, global adherence to agreed norms should be promoted through capacity-building initiatives and widespread educational programs. These efforts can help states, particularly those with limited resources, to internalize and operationalize the legal frameworks and technical safeguards necessary for cyberspace governance. Second, states should be encouraged to adopt transparent policies, which include effective incident reporting mechanisms. Such transparency builds trust, enhances accountability, and facilitates timely responses to cyber incidents. Finally, fostering research into vulnerabilities of critical infrastructures, such as undersea cables and satellites, is essential. Coordinated international efforts to develop protocols for managing cyber risks and responding to attacks will ensure the resilience of global connectivity.

It is recommended for states to prioritize the implementation of the confidence-building measures (CBMs) established by the UN Group of Governmental Experts to promote trust and prevent conflicts

in cyberspace. These measures, including information-sharing, establishing points of contact, and promoting transparency in cyber operations, play a critical role in reducing risks of misperception and escalation. Adherence to CBMs fosters collaboration, enhances mutual understanding, and strengthens international stability in the digital domain. By committing to these practices, states can support a secure and predictable cyber environment, reinforcing the broader framework of international law and contributing to peaceful interactions in an increasingly interconnected world.

ACKNOWLEDGMENT

This work was supported by Shota Rustaveli National Science Foundation of Georgia (SRNSFG) - CG-24-220.

REFERENCES

1. UN GGE 2013 Report: United Nations, Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, A/68/98 (24 June 2013). Available at: https://digitallibrary.un.org/record/752462;
2. UN GGE 2015 Report: United Nations, Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, A/70/174 (22 July 2015). Available at: https://digitallibrary.un.org/record/799853
3. European Council, "Declaration on a Common Understanding of International Law in Cyberspace," Brussels, November 18, 2024, Document 15833/24, CYBER 334, COJUR 111, COPS 622.