SIOI
UNA Italy
OSSERVATORIO
sulle attività delle organizzazioni internazionali e sovranazionali, universali e regionali, sui temi di interesse della politica estera italiana

Reflexions on the hostile activities in cyberspace and the international legal landscape promoted by the United Nations

Annita Larissa Sciacovelli
Ricercatrice di Diritto Internazionale, Università degli Studi di Bari Aldo Moro

1. The Cyber Threat Landscape

In July 2024, the United Nations (UN) Open-ended Working Group on the Security and Use of Information and Communications Technologies (OEWG) will start working on its third annual progress report, which will be submitted to the UN General Assembly (UNGA)[1].

The OEWG President has already sent the Zero Draft, dated May 29, 2024, to UN Member States for public discussion[2]. This draft outlines the evolution of the eleven voluntary non-binding norms of responsible state behaviour in the use of Information and Communications Technologies (UN non-binding norms) and includes regulatory proposals. These norms were adopted by consensus by the UN Group of Governmental Experts (GGE) in 2015 and later by the OEWG[3]. This decalogue concerns: the maintenance of international peace and security in line with the objectives and principles of the UN; the ban on using state territory for internationally prohibited activities; the peaceful use of Information and Communications Technologies (ICT) in compliance with human rights; the respect for state sovereignty; the peaceful resolution of international disputes and the prohibition of interference in the internal, and non-intervention in the internal and external affairs of states through ICT.

The Zero Draft prompts important considerations about the application of these norms in today's digital environment[4]. This environment is a challenging geopolitical

[1]This Publication was produced with the co-funding of the European Union - Next Generation EU: NRRP Initiative, Mission 4, Component 2, Investment 1.3 - Partnerships extended to universities, research centres, companies and research D.D. MUR n. 341 del 15.03.2022 – Next Generation EU (PE0000014 – "SEcurity and Rights In the CyberSpace – SERICS" - CUP: H93C22000620001). https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/Letter_from_OEWG_Chair_29_May_2024.pdf.

[2] Letter from the Chair of the Open-Ended Working Group on Security of and in the Use of Information and Communications Technologies, 2021-2025, February 20, 2024, p. 6.

[3] GEE, *Report 2015*, UN Doc. A/RES/70/237; OEWG, *Report 2022*, UN Doc. A/77/275.

[4] H.S. Lin, *Offensive Cyber Operations and the Use of Force*, in *Journal of National Security Law and Policy*, 2010, p. 4; M. Schmitt, *Tallinn Manual on the International Law Applicable to Cyber Warfare*, Cambridge, 2013; M. Roscini, *Cyber Operations and the Use of Force in International Law*, Oxford, 2014; K. Kittichaisaree, *Public International Law of Cyberspace*, Cham, 2017; D. Mandrioli, *Il caso* Wannacry*: il fenomeno dei* Cyber Attacks *nel contesto della responsabilità internazionale degli Stati*, in *La Comunità Internazionale*, 2018, p. 473; A. Bonfanti, *Attacchi cibernetici in tempo di pace: le intrusioni nelle elezioni presidenziali statunitensi del 2016 alla luce del diritto internazionale*, in *Rivista di diritto internazionale*, 2019, p. 212; N. Tsagourias, R. Buchan (eds.), *Research Handbook on International Law and Cyberspace*, Cheltenham/Northampton, 2021; G. Della Morte, *Limiti e prospettive del diritto internazionale del cyberspazio*, in *Rivista di diritto internazionale*, 2022, p. 9; M.C. Vitucci, *Le ciberoperazioni e il diritto internazionale, con alcune considerazioni sul conflitto ibrido russo-ucraino*, in *La Comunità Internazionale*, 2023, p. 7; A. Stiano, *Attacchi informatici e responsabilità internazionale degli Stati*, Napoli, 2023.

arena where the malicious use of IC by state and non-state actors significantly impacts national and international peace and security[5].

The current cyber threat landscape is highly dynamic, constantly evolving, and complex. It is continuously redefined by the nature of hostile activities in cyberspace and the increasing number and variety of threat actors[6]. Hostile activities are growing in both scale and intensity, partly due to the offensive use of emerging technologies such as Artificial Intelligence (AI) and, in the near future, Post-Quantum Computing[7]. AI is used to create new vectors of attack by scanning the ICT systems of public and private critical infrastructures to find vulnerabilities, thereby expanding their surface of attack.

These malicious cyber operations have far-reaching impacts on public safety and national security, potentially they may cause cascading effects at national, regional, and global levels. They can include pre-positioning malware for exploitation in potential conflicts, which increases the risk of escalation and conflict both in cyberspace and beyond.

These operations can even exceed the threshold of the prohibition on the use of force, as stated in Article 2, para. 4, of the UN Charter, which prohibits "the threat or use of force against the political independence or territorial integrity of any state, or in any other manner inconsistent with the purposes of the United Nations"[8].

Most hostile activities conducted so far, such as those in 2007 against Estonia, in 2019 against Georgia, and in 2014 and 2022 against Ukraine, do not violate the prohibition on the use of force or the law of armed conflict[9]. Instead, they violate the principles of non-intervention or of territorial sovereignty of the targeted states because ofte cyber operations are part of a composite operation. Therefore, they need to be addressed differently.

As cyberspace becomes increasingly crucial for the maintenance of international peace and security, as acknowledged by the UN Security Council in its informal meeting on the "Evolving cyber threat landscape and its implications for the maintenance of international peace and security" [10], the aim of this paper is to explain the landscape of hostile activities and of actors in cyberspace in the light of the OEWG's contribution to the evolving framework of the UN non-binding norms. Specifically, we will analyse the

---

[5] S. Haataja, *Cyber Operations Against Critical Infrastructure Under Norms of Responsible State Behaviour and International Law*, in *International Journal of Law and Information Technology*, 2022, p. 423.

[6] https://www.securitycouncilreport.org/atf/cf/%7B65BFCF9B-6D27-4E9C-8CD3-CF6E4FF96FF9%7D/arria%20formula%20on%20cybersecurity.pdf.

[7] https://www.microsoft.com/en-us/security/security-insider/microsoft-digital-defense-report-2023.

[8] M.C. Waxman, *Cyber Attacks as "Force" Under UN Charter Article 2(4)*, in *International Law Studies*, 2011, p. 43, https://scholarship.law.columbia.edu.

[9] G. Nakashidze, *Cyberattack against Georgia and International Response: Emerging Normative Paradigm of 'Responsible State Behavior in Cyberspace'?,* 2020, in https://www.ejiltalk.org; I. Zahra, I. Handayani, D.W. Christianti, *Cyber-attack in Estonia: A New Challenge in the Applicability of International Humanitarian Law*, in *Yustisia*, 2021, p. 48; M. Orenstein, *Russia's Use of Cyberattacks: Lessons from the Second Ukraine War*, in *Foreign Policy Research Institute*, 2022, https://www.fpri.org.

[10] https://www.stimson.org/2024/un-security-council-cyber-threats-to-international-security/.

action-oriented proposals of the Zero Draft and their potential role in reducing risks to international peace and security.

2. Hostile Activities and Hostile Actors in Cyberspace

Malicious cyber operations are conducted using worms, logic bombs, malware, trojans, and bots to inflict ransomware, distributed denial-of-service (DDoS) attacks, cyber espionage, or to deploy wipers to disrupt and destroy large datasets in critical sectors[11]. These activities can cause damage in both the digital and physical worlds, across various jurisdictions, often targeting critical and strategic infrastructures within national cybersecurity perimeters. Such operations undermine the functioning of essential services like national healthcare systems, banking and financial services, large automated industrial complexes in the energy and manufacturing sectors, transportation, telecommunications, water plants, and recently undersea cables and orbit communication systems.

From a financial perspective, cybercrime is the world's third largest economy. Its costs reached $8.44 trillion in 2022 and, according to data from the FBI and IMF, are expected to surge to $23.84 trillion by 2027[12].

Malicious actors in cyberspace can be divided into two categories: states and non-state actors. States are developing ICT capabilities for military purposes and have used them in international conflicts (e.g., Russia and Ukraine), regional rivalries (e.g., India and Pakistan), and conflicts (e.g., Israel and Hamas)[13]. States often use their military and intelligence apparatus to organize cyber hostile operations, though they prefer to act through groups of professional criminal hackers, known as proxies (Albania)[14].

Non-state actors include individuals, groups, companies, or private military and security companies that now demonstrate ICT capabilities that previously were only available to states. This shift is partly due to the cheap commercial availability of ransomware tools (ransomware-as-a-service), leading to the privatization of offensive

---

[11] N.M. Schmitt, L. Vihul, *Tallin Manual 2.0, The International Law Applicable to Cyber Operations*, Cambridge, 2017.

[12] https://www.weforum.org/agenda/2024/01/cybersecurity-cybercrime-system-safety/.

[13] M. Baezner, *Hotspot Analysis: Regional Rivalry Between India-Pakistan: Tit-for-tat in Cyberspace*, Center for Security Studies, ETH Zurich, 2018, https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2018-04.pdf; T. Mimran, *Israel-Hamas 2023 Symposium, Cyberspace, the Hidden Aspect of the Conflict*, https://lieber.westpoint.edu/cyberspace-hidden-aspect-conflict/. On the nature of the conflicts between Israel and Hamas, and between Israel and Palestine, see the press statement of May 20, 2024 of the International Criminal Court Prosecutor, Karim A.A. Khan KC, *Applications for Arrest Warrants in the Situation in the State of Palestine,* 2024, where he announces the intent to seek arrest warrants for Palestinian and Israeli figures and he affirms "[M]y Office submits that the war crimes alleged in these applications were committed in the context of an international armed conflict between Israel and Palestine, and a non-international armed conflict between Israel and Hamas running in parallel", https://www.icc-cpi.int. The statement is based on the Report of the Panel of Experts in International Law of 2024 that characterized the hostilities between Hamas and Israel as "sufficiently intense to reach the threshold of a non-international armed starting […] at the latest, on 7 October 2023", https://www.icc-cpi.int/sites/default/files/2024-05/240520-panel-report-eng.pdf. J.B. Quigley, *Karim Khan's Dubious Characterization of the Gaza Hostilities*, 2024, https://www.ejiltalk.org.

[14] A.L. Sciacovelli, *Taking Cyber-Attacks Seriously: the (likely) Albanian Cyber Aggression and the Iranian Responsibility*, in *OSORIN*, 2023.

cyber capabilities. Non-state actors can be terrorists, criminal groups, hacktivists, patriotic hackers, Advanced Persistent Threats (APTs), and cyber mercenaries. The latter are private actors engaged by states to conduct offensive or defensive cyber operations to weaken the military capacities of adversary forces or undermine the integrity of other states' territories[15].

Criminal hackers typically pursue economic and political goals. Economically motivated cybercrimes can generate profits from hundreds to millions of dollars, enabling their self-financing. Politically motivated cyber activities often reflect the geopolitical positions of hacktivist groups or states on specific issues, such as the conflict in Ukraine or the conflicts between Israel and Hamas.

From the European Union (EU) perspective, a key trend in cyberspace is the blurring of lines between state-sponsored and criminal or financially motivated actors[16]. States increasingly act through non-state actors, who have assumed a prominent role in modern conflicts. This strategy allows states to elude international responsibility for malicious activities committed by non-state actors, given the high evidential standards required for attribution in international law[17]. Additionally, the anonymity provided by cyberspace, especially using *Onion Router* (*Tor*) and *Virtual private networking* (*VPN*), makes it difficult to identify both the individual responsible for the malicious activities and the sponsoring state[18]. The use of these tools can lead to misattribution, as in the case of *false flags operations*, where a target state reacts against an incorrect party[19]. The cited difficulties in collecting the digital evidence needed for attribution in international law require alternative solutions to prevent states from orchestrating cyber proxy wars.

---

[15] Report of the UN Working Group on the use of mercenaries as a means of violating human rights and impeding the exercise of the right of peoples to self-determination, July 15, 2021, UN Doc. A/76/151.

[16] https://www.eeas.europa.eu/delegations/un-new-york/eu-statement-%E2%80%93-un-security-council-arria-formula-meeting-cyber-security_en.

[17] Articles 5 and 8 of the *Draft Articles on the Responsibility of States for Internationally Wrongful Acts*, *Yearbook of the International Law Commission*, 2001, vol. II, part 2; Rule 15, *Tallinn Manual 2.0*, cit.; *Symposium on Cyber Attribution*, in *AJIL Unbound by Symposium*, 2019, www.cambridge.org; J. Christoph, *Cyber Warfare*, in *Max Planck Encyclopedia of Public International Law*, Oxford, 2015, p. 1; N. Tsagourias, M.D. Farrell, *Cyber Attribution: Technical and Legal Approaches and Challenges*, 2018, https://sites.tufts.edu.

[18] For The NATO Cooperative Cyber Defence Centre of Excellence, *Mitigating Risks arising from False-Flag and No-Flag Cyber Attacks*, https://ccdcoe.org: "[I]t is not enough to just locate a source IP address (unless looking solely at active defence): the identity of the attackers must be determined, as well as the parties they were acting on behalf of must also be unmasked"; K. Mačák, *Decoding Article 8 of the International Law Commission's Articles on State Responsibility: Attribution of Cyber Operations by Non-State Actors*, in *Journal of Conflict and Security Law*, 2016, p. 405.

[19] E.M. Mudrinich, *Cyber 3.0: The Department of Defense Strategy for Operating in Cyberspace and the Attribution Problem*, in *Air Force Law Review*, 2012, p. 167; K.E. Eichensehr, *The Law & Politics of Cyberattack Attribution*, in *University of California Los Angeles Law Review*, 2020, p. 67; A. Kastelic, *Non-Escalatory Attribution of International Cyber Incidents: Facts, International Law and Politics*, 2022, https://unidir.org.

3. The UN Contribution to the Evolution of the International Legal Landscape of Cyberspace

To address the multifaceted nature of cyber threats, the UN has consistently worked to build a consensus on the applicability of international law to activities in cyberspace. Significant contributions in this sector come from the GGE, whose reports were agreed upon by consensus in 2013, 2015, and 2021, and the OEWG, whose reports were adopted in 2021, 2022, and 2023[20]. These two working groups, established by the UNGA, have similar mandates, although different geopolitical origins. They promote the UN non-binding norms of responsible state behaviour, based on international law, particularly the UN Charter, "which is applicable and is essential to maintaining peace, security and stability in the ICT environment"[21].

The OEWG's mission is to contribute to the creation of an open, safe, secure, stable, accessible, and peaceful ICT environment to maintain international peace and security by proposing an open, non-exhaustive list of rules, norms, principles of international law, and confidence-building measures and consensus-building[22].

The OEWG's confidence-building measures intend to operationalize the UN non-binding norms, particularly regarding sovereignty, non-intervention in internal and external state affairs, peaceful settlement of disputes, state responsibility, due diligence, and the application of international humanitarian law in armed conflicts[23]. States recognize the importance of these discussions within the OEWG's yearly sessions as they lead to the common understandings on how international law applies to ICT use, increasing the predictability of state behaviour, reducing the risk of miscalculation in attributing cyber activities, and clarifying the consequences of unlawful state behaviour[24].

4. Recent Proposals for Confidence-Building Measures to Counter Malicious Activities in Cyberspace

The OEWG has put forth several concrete and actionable proposals regarding the interpretation and application of international law principles in cyberspace, as outlined in the Zero Draft. These proposals serve as a practical checklist for implementing the UN non-binding norms.

Beginning with the notion of state sovereignty, which extends to jurisdiction over ICT infrastructure within its territory, these proposals advocate for states to apply existing

---

[20] GEE, *Report 2013*, UN Doc. A/68/243; *Report 2015*, UN Doc. A/70/174; *Report 2021*, UN Doc. A/73/512.

[21] OEWG, *Report 2021*, UN Doc. A/75/816, Annex I, para. 7.

[22] https://docs-library.unoda.org/Open Ended_Working_Group_on_Information_and_Communication_Technologies_(2021)/Letter_from_OEWG_Chair_27_July_2023.pdf.

[23] Letter of the OEWG Chair, fnt 2, para. 35; International committee of the Red Cross, *Cyber Operations During Armed Conflicts*, 2021, https://www.icrc.org.

[24] GEE, *Official Compendium of Voluntary National Contributions on the Subject of How International Law Applies to the Use of ICTs by States*, 2021, 84, UN Doc. A/76/136.

international law obligations to protect their ICT infrastructure from cyber threats[25]. Such measures are crucial for ensuring the prompt addressing of ICT vulnerabilities, thereby reducing the risk of exploitation by malicious actors. Timely discovery, disclosure, and addressing of ICT vulnerabilities can prevent harmful practices, foster trust and confidence, and reduce threats to international security and stability.

Furthermore, in accordance with the principle of non-intervention, states must refrain from intervening, directly or indirectly, in the internal and external affairs of other states also through ICT.

Aligned with the principle of state sovereignty, Norm C of the UN non-binding norms emphasizes that states should not knowingly allow their territory to be used for wrongful acts via ICT. Under its corollary, the principle of *due diligence principle*, states should "not conduct or knowingly support ICT activity contrary to its obligations under international law that intentionally damages critical infrastructure or otherwise impairs the use and operation of critical infrastructure to provide services to the public" of other states[26]. In the event of malicious cyber activities occurring within or transiting through a state's territory, the state is expected to take reasonable, proportionate, and effective measures to halt such activities, consistent with international law. However, it is not expected that the state should monitor all ICT activities within its territory.

Discussions among states also revolve around how to address the transborder nature and anonymity of ICT operations under international law, particularly concerning when malicious activities reach the threshold of the use of force and, eventually, constitute an armed attack. States are encouraged to respond to requests for assistance and mitigation from other states whose critical infrastructure has been targeted by malicious activities, especially if they pose threats to international peace and security.

States are also asked to facilitate the tracing of hostile activities on critical information infrastructures and, when appropriate, disclose this information to other states. In case of an ICT incident, the affected state should notify the state from which the hostile activity is emanating, although the receiving of the notification does not imply the acknowledgment of the responsibility on the receiving state.

In this context, the paper entitled "Draft Elements for the Open-Ended Action-Oriented Permanent Mechanism on ICT Security in the Context of International Security" proposed by the OEWG's Chair deals with the establishment of a Permanent Mechanism on ICT Security[27]. This mechanism, to be submitted for states' approval in July 2024,

---

[25] Norm G of the UN non-binding norms. A.A. Donis, *International Law on Cyber Security in the Age of Digital Sovreignty*, in *E-Int relations*, 2020, www.e-ir.info; A. Kastelic, *International Cyber Operations*, 2021, p. 1, https://www.unidir.org.

[26] Norm F of the UN non-binding norms. R.J. Buchan, *Cyberspace, Non-State Actors and the Obligation to Prevent Transboundary Harm*, in *Journal of Conflict & Security Law*, 2016, pp. 429-453.

[27] https://docslibrary.unoda.org/OpenEnded_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/Letter_from_OEWG_Chair_1_May_2024_0.pdf. See N.M. Schmitt, *In Defense of Due Diligence in Cyberspace*, in *Yale Law Journal Forum*, 2015, p. 68; M.N. Schmitt, L. Vihul, Rule 6, *Tallin Manual 2.0*, cit., p. 30; I. Couzigou, *Securing Cyber Space: The Obligation of States to Prevent Harmful International Cyber Operations*, 2018, p. 37, https://aura.abdn.ac.uk.

will foster regular institutional dialogue to develop the application of international law in ICT use, particularly in responding to malicious cyber activities attributable to states. It is expected to serve as a scenario-case discussion to address such activities in accordance with states' obligations under international law.

Regarding the application of the obligation of peaceful solutions of disputes between states (Article 2, para. 3, UN Charter), the OEWG proposes the establishment of a global, inter-governmental Points of Contact (POC) directory. This directory aims to facilitate secure and direct communications between states during urgent and significant ICT incidents, helping to build confidence, de-escalate tension, and prevent misunderstandings and misperceptions that could lead to international crisis.

The manager of the POC directory will be the UN Office for Disarmament Affairs (UNODA) and the Zero Draft suggests that all interested states should nominate their national POCs. Standardized templates could further optimize direct communications between states during significant ICT incidents through the POC directory; it could ensure clarity and timeliness while maintaining flexibility and voluntariness especially in cases of urgent request.

Another notable initiative is the creation of a Global Cyber Security Cooperation Portal (GCSCP), which could complement the proposal for a repository of best practices in ICT security capacity-building. This measure aims to address the lack of awareness of existing and potential threats and the lack of technical capacities among states to detect and defend against malicious ICT activities, especially in case of developing countries.

5. Concluding remarks

The evolving cyber threat landscape presents significant challenges to international peace and security. The increasing sophistication and frequency of cyber-attacks by state and non-state actors highlight the urgent need for a robust and adaptive international legal framework. As cyber operations continue to blur the lines between conventional and unconventional warfare, the international community must work together to address these emerging threats.

Moreover, the challenges of attribution, accountability, evidentiary issue require innovative and cooperative solutions[28]. The complexity of cyberspace demands that states not only strengthen their defensive capabilities but also engage in proactive measures to prevent cyber incidents. By adopting and operationalizing the proposed confidence-building measures, states can enhance the predictability of their behaviour in cyberspace, thereby reducing the risk of miscalculations and conflicts.

[28] M. Roscini, *Evidentiary Issues in International Disputes Related to State Responsibility for Cyber Operations*, in *Texas International Law Journal*, 2015, p. 233; M. Finnemore, D.B. Hollis, *Beyond Naming and Shaming: Accusations and International Law in Cybersecurity*, 2019, papers.ssrn.com.

In this scenario, the OEWG plays a crucial role in shaping this framework by promoting the implementation of voluntary non-binding norms of responsible state behaviour in cyberspace and crafting the essence of cyber diplomacy.

Key proposals from the Zero Draft, such as enhancing state sovereignty over ICT infrastructure, ensuring non-intervention, and promoting due diligence, provide a solid foundation for building trust and cooperation among states. These measures, coupled with the establishment of a global Points of Contact directory and the reaffirmation of international humanitarian law in cyberspace, offer practical steps toward reducing the risks of cyber conflicts and their humanitarian impact.

The Zero Draft of the OEWG's third annual progress report underscores the necessity of the application of these norms and proposes actionable measures to mitigate cyber threats. By fostering dialogue and consensus among UN Member States, the OEWG aims to enhance cyber international peace and security.

In conclusion, the OEWG's initiatives represent significant progress towards establishing a secure, stable, and peaceful ICT environment especially because the proposed solutions are sustainable, effective, and affordable. By embracing these proposals and fostering greater collaboration, UN Member States can ensure that the digital realm contributes to international peace and security rather than becoming a source of conflict and instability. However, the development of international cyber law faces significant challenges, and several critical factors hinder progress. For instance, states are reluctant to formalize the UN's non-binding rules into an international treaty due to geopolitical rivalries, to concerns about protecting fundamental rights and freedoms, and to unclear national positions on how international law applies to ICT activities[29].The path forward requires sustained commitment, cooperation, and innovation to navigate the complexities of the cyber threat landscape and to protect the integrity and stability of our interconnected world.The international community stands at a critical juncture in the governance of cyberspace next July and for the next decades.

Giugno 2024

[29] P. Roguski, *Application of International Law to Cyber Operations: A Comparative Analysis of States' views*, Policy Brief, The Hague Program for Cyber Norms, 2020, https://www.thehaguecybernorms.nl.