United Nations Working Group Approves Cybersecurity Report: What is it and What are the Implications?

Written by Christina G. Hioureas, Tracy Roosevelt, Colin J. Zick, Christopher Escobedo Hart

April 27, 2021

On 12 March 2021, the United Nations Open-ended Working Group ("**OEWG**"), established by General Assembly Resolution 73/27 and consisting of all United Nations Member States, adopted by consensus its Final Substantive Report on cybersecurity ("**Report**"). Adopted against the background of the COVID-19 pandemic and noting the need to protect healthcare and informational infrastructure,[1] the Report provides recommendations for peaceful use of information and communications technologies ("**ICT**s") and has been heralded as "the first time that a process open to all countries has led to agreement on international cybersecurity."[2]

While not legally binding, the Report provides a foundation for future negotiations on the progressive development of international law in connection with cybersecurity.[3] It acknowledges areas of consensus and makes recommendations for future cooperation, including:

1. **Existing and Potential Threats** – States agreed that there are increasing concerns about malicious use of ICTs for the maintenance of peace and security, human rights, and development.
2. **Rules, Norms and Principles for Responsible State Behavior** – without defining the scope of these norms, it was confirmed that voluntary, non-binding norms of responsible State behavior can reduce risks to international peace and security and contribute to the prevention of conflict.
3. **International Law** – States, on a voluntary basis, agreed to continue to inform the UN Secretary General of their views on the application of international law to ICTs, build capacity in this area, and continue to study how international law applies to ICTs.
4. **Confidence-building Measures ("CBMs")** – It was agreed that transparency, cooperative and stability measures can contribute to preventing conflicts; and that voluntary CBMs can serve as the first step in addressing mistrust and misunderstandings between States. States should continue to inform the Secretary General of their views in this area, and voluntarily engage in transparency measures by sharing relevant information and lessons.
5. **Capacity-building** – States concluded that capacity building is critical to the ability of States to respond to malicious ICT activity, and that they should be guided by (i) a sustainable, evidence-based, politically neutral and transparent process; (ii) partnerships driven by trust; (iii) respect for human rights, fundamental freedoms, gender sensitivity, inclusivity, and non-discrimination, as well as respect for confidentiality of sensitive information.
6. **Regular Institutional Dialogue** – it was agreed that States continue to actively participate in regular institutional dialogue under the auspices of the UN on ICTs.

These principles lay a foundation for exchange of views on ICTs, building on the rich discussion that took place during this process, and including the possibility of future legally binding obligations. The work of the OEWG has taken place in parallel with technical work undertaken by the Group of Governmental Experts, a 25-member group that has been issuing reports on complex tech issues since 2019.

One issue highlighted in the Report was the challenge of regulating ICTs while acknowledging that they are already regulated to some extent by international law. The OEWG reaffirmed "[s]pecific principles of international law" including, "State sovereignty; sovereign equality; the settlement of international disputes by peaceful means in such a manner that international peace and security and justice are not endangered; refraining in their international relations from the threat or use of force against the territorial integrity of political independence of any State, or in any other manner inconsistent with the purposes of the United Nations; respect for human rights and fundamental freedoms; and non-intervention in the internal affairs of other States." States recalled that while ICTs are not specifically

addressed under international law, such law can develop through *opinio juris* and State practice.[4] Some member States expressed skepticism as to whether some States may be using the negotiations to dilute international law standards by, for example, negotiating the exclusion of how international humanitarian law limits the use of ICT capabilities during armed conflict from the Report.[5]

The Report is timely in light of the pandemic, and its substance has been added to the provisional agenda for the seventy-sixth session of the General Assembly. More than 50 member States support a proposal for a cyber Programme of Action, and it has been speculated that there could be a Resolution requesting a negotiating mandate for it at the seventy-sixth session of the General Assembly's First Committee this year. Even if there is not immediately a Resolution, the Report is the first step in a longer evolution of norms for ICTs and cybersecurity. Additionally, a new working group will further continue the discussion on ITCs when it commences its mandate in 2021. That group will report to the General Assembly in 2025.[6]

---

[1] Final Substantive Report, Open-ended working group on developments in the field of information and telecommunications in the context of international security, para. 26 (10 March 2021), https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf ("that the COVID-19 pandemic has accentuated the importance of protecting healthcare infrastructure including medical services and facilities through the implementation of norms addressing critical infrastructure, such as those affirmed by consensus through UN General Assembly resolution 70/237.")

[2] Josh Gold, Unexpectedly, All UN Countries Agreed on a Cybersecurity Report. So What? Council on Foreign Relations, Blog Post (18 Mar. 2021), *available at* https://www.cfr.org/blog/unexpectedly-all-un-countries-agreed-cybersecurity-report-so-what.

[3] Delegations also issued official "explanation of positions" in writing since the meeting was held in a hybrid in-person and virtual format. Letter of the Chair on preparations for the adoption of the OEWG report (11 March 2021), https://front.un-arm.org/wp-content/uploads/2021/03/210311-OEWG-Chairs-letter-in-preparation-of-the-adoption-of-the-Groups-report.pdf. *See* Compendium of statements in explanation of position on the final report (25 Mar. 2021), *available at* https://front.un-arm.org/wp-content/uploads/2021/04/A-AC.290-2021-INF-2.pdf.

[4] Chair's Summary, Open-ended Working Group on Developments in the Field of International and Telecommunications in the Context of International Security, Third substantive session, para. 11 (10 March 2021).

[5] David Ignatius, "Opinion: How Russia and China are attempting to rewrite cyberworld order," *Washington Post* (30 March 2021).

[6] G.A. Res. A/C.1/75/L.8/Rev.1, *Developments in the field of information and telecommunications in the context of international security* (26 Oct. 2020), https://www.undocs.org/en/A/C.1/75/L.8/Rev.1.

RELATED INDUSTRIES

- Sovereign States

RELATED PRACTICES

- Cybersecurity Incident Response
- Privacy & Data Security
- United Nations
