insights

Volume: 25 Issue: 14

By: **Adina Ponta**

July 30, 2021

Responsible State Behavior in Cyberspace: Two New Reports from Parallel UN Processes

Introduction

There are currently two major United Nations (UN) sponsored initiatives that address the future of international security in cyberspace: the UN Group of Governmental Experts on Advancing Responsible State Behavior in Cyberspace in the Context of International Security (GGE) and the Open-Ended Working Group on Developments in the Field of Information Telecommunications in the Context of International Security (OEWG). Based on the OEWG's first report and the recent GGE report, as well as public submissions made by states in the context of both groups' work, this *Insight* analyses the most relevant proposals that have been suggested to promote responsible state behavior in cyberspace.

What are the GGE and the OEWG?

The GGE is a UN mandated working group tasked to examine the impact of ICT developments in information telecommunications (ICTs) on national security and military affairs. Since its debut in 2004, six working groups have been established. The latest GGE concluded its work in May 2021 by adopting a consensus report. In previous years, the GGE's core achievements were recognizing that international law applies to cyberspace (2013) and introducing non-binding and voluntary norms of responsible state behavior (2015). Negotiations failed during the 2016–17 round, however, and the group did not produce a report. Experts disagreed on questions about the concrete application of international law, particularly international humanitarian law (IHL), countermeasures, and the right to self-defense in cyberspace. The GGE reports are adopted by the UN General Assembly, meaning that while they have no binding power, their normative influence is significant.

In the aftermath of the 2017 impasse and subsequent disagreement on a future format for consultations, the General Assembly approved in 2018 a Russian-sponsored resolution calling for the establishment of the OEWG and a U.S.-sponsored resolution calling for the establishment of a new GGE.[1] These twin processes have since worked in parallel, with quasi-overlapping mandates but different membership.

The 2019-2021 GGE comprised experts from 25 member states on the basis of equitable geographical distribution, including the five permanent members of the Security Council. Its mandate was to address the applicability of international law to cyberspace, norms, rules and principles, confidence building measures, and capacity building. The first OEWG was open to all interested states. Unlike the GGE, which has held its meetings behind closed doors, the OEWG deliberated in public and states could submit public contributions to its deliberations (although the transparency of the process declined in the wake of the COVID-19 pandemic). In December 2020, the OEWG's mandate was renewed for 2021/2025.[2]

The OEWG report

The OEWG's final report was unanimously adopted by the 68 participating states in March 2021, becoming the first report on cybersecurity of this scale adopted with direct governmental participation.[3] Unlike previous GGE reports, the OEWG clearly structured the topics around which states achieved consensus. Under the UNGA 2018 resolution, it was tasked with discussing the following substantive issues:

1. ***Existing and potential threats*****.** The report recognizes the amplified frequency, sophistication, and diversity of harmful ICT incidents, as well as the increased likelihood of using cybermeans in future conflicts—including by "terrorists and criminal groups"—and their potentially devastating impacts. For example, the rising number of hostile cyberoperations jeopardizes essential public services "such as medical facilities, financial services, energy, water, transportation, and sanitation." In the first round of contributions, a number of states also emphasized the threat of disinformation and foreign interference against electoral processes; however, the final report only contains a brief reference connecting election interference to the underlying critical infrastructure (CI) and critical information infrastructure.

2. ***Rules, norms and principles****.* This section emphasizes both the relevance and the limits of voluntary non-binding norms for international peace, security, and stability. While norms contribute to more predictable behavior and the prevention of conflict, they are unable to replace or modify binding "States' obligations or rights under international law"

(¶ 25). The OEWG recommends the development and implementation of norms of responsible state behavior and the exchange of best practices on the protection of critical infrastructure, expressly mentioning supply chain security, but its wording on this point is broad. The report also highlights states' duties to prevent the proliferation of malicious tools and use of harmful hidden functions, by encouraging the reporting of vulnerabilities. Additionally, the section emphasizes the "norm on protecting the public core of the internet," as suggested by the Global Commission for Stability of Cyberspace.

3. ***International Law*****.** The report reaffirms the previous GGE statement that international law, including the UN Charter, is applicable to cyberspace. The OEWG also expressly recognizes dispute settlement mechanisms provided by the UN Charter, encouraging states to "seek the settlement of disputes by peaceful means such as negotiation, enquiry, mediation, conciliation, arbitration, judicial settlement, and resort to regional agencies or arrangements, or other peaceful means of their own choice" (¶ 35). The report concludes that the most effective way to reach common ground on the concrete application of international law to the ICT environment is through regular exchange of views and practices, and identification of specific international law issues that require in depth conversations, under the auspices of the UN and the Secretary General. Overall, the report refrains from specifying concrete international law branches that might apply, the prospect of which had raised high expectations. The absence of any references to IHL in the final report, for instance, has drawn criticism. Several states (Cuba, China, Belarus) oppose the application of IHL, fearing that doing so will legitimize the militarization of cyberspace. In response to a submission by the International Committee for the Red Cross, the OEWG Chair noted the need to further clarify "certain questions on how international law applies to the use of ICTs [including] questions relevant to how the principles of international humanitarian law, such as principles of humanity, necessity, proportionality, distinction and precaution, apply to ICT operations."[4]

4. ***Confidence building measures (CBMs)*****.** CBMs are policy tools aimed at mitigating threats, building trust and communication channels, and have been traditionally promoted in tackling international security issues, such as nuclear non-proliferation or disarmament. The report recommends that states voluntarily identify appropriate CBMs in the cyberspace context and cooperate on their implementation. States agreed to voluntarily engage in transparent CBM mechanisms, such as exchanges of information, good practices, and lessons learned about implementation, via established national points of contacts and diplomatic channels.

5. ***Capacity building*****.** The report outlines the principles of sustainable and purposeful capacity building, which should be specific and results-oriented, evidence-based,

politically neutral, transparent, accountable, and undertaken with full respect for the principle of state sovereignty. The report ignores existing multi-stakeholder efforts in this area, however, such as those promoted by the Organization for Security and Co-operation in Europe (OSCE) and several European initiatives.[5]

6. ***Regular institutional dialogue*****.** The report recommends states' continuous active participation in regular institutional dialogue under the auspices of the UN. Likeminded states and the European Union (EU) expressed their support for a newly created "Programme of Action," meant to be a permanent UN forum to consider ICTs in the context of international security and end the parallel GGE and OEWG processes. The wide support for this framework is more promising for concrete actions, stronger commitments, and strengthened accountability.

The product delivered by the OEWG is split between the substantive Final Report and the Chair's summary, which contains issues on which participants could not reach consensus (e.g., attribution, international humanitarian law, a clear integration of election processes in critical infrastructures, etc.). Some commentators have suggested that the OEWG report lacks substance for failing to achieve consensus on these points, while others have praised it for creating a path to greater institutional dialogue and for affirming the GGE's earlier work.

The 2021 GGE Report

Shortly after the OEWG's final round, the GGE released an advance copy of its report, confirming the diplomatic progress on responsible behavior in cyberspace at the UN.[6] Given the failure of the last GGE, including the aftermath of severe hostile cyber operations against GGE members, the Working Group's efforts to reach consensus and compromise on key issues represent important progress.

The released document is broken down into seven sections, which are almost overlapping with the OEWG report, given the similarity of their mandates. Unlike the OEWG, perhaps the most substantive step forward for the GGE is its acknowledgment that IHL applies to cyber operations during an armed conflict, including by evoking the fundamental principles of humanity, necessity, proportionality, and distinction. As disagreement still remains on concrete interpretation of IHL principles, the GGE recognized the need for further dialogue on qualification of key terms in the cyber context. The latest GGE round also demonstrated that states are still hesitant to determine the nature of due diligence obligations. Derived from the principle of state sovereignty, due diligence entails states' duties to ensure that the territory or cyber infrastructure under their control is not used for operations that affect the rights of – and produce serious adverse consequences for – other states. While the 2013 and 2015 GGE rounds addressed due diligence as a voluntary, non-binding norm of responsible state behavior, the 2021 report defines it as a broad and common-sense expectation "that a State will take reasonable steps within its capacity to end the ongoing activity in its territory through means that are proportionate, appropriate and effective and in a manner consistent with international and domestic law." (para. 36 a) The GGE's emphasis on the reasonable character of this duty ("it is not expected that States could or should monitor all ICT activities within their territory") and on providing assistance for states lacking requisite capacity offers hope that states will eventually recognize this duty as an international law rule.

Unlike the OEWG report, the GGE's 2021 report expands on principles of international law that might be relevant in cyberspace. Building on the 2015 report, which mentions state commitment to sovereign equality, the GGE's 2021 report includes a prohibition of the threat or use of force against the territorial integrity or political independence of another state, respect for human rights and fundamental freedoms, and nonintervention in the internal affairs of other states. Like the OEWG report, however, it underscores the vulnerability of critical infrastructure in the face of hostile cyberoperations. After the EU emphasized during the OEWG consultations, that "critical infrastructures are no longer confined to the borders of States, but are increasingly becoming transnational and interdependent," both the GGE and the OEWG report highlight the lack of protection and regulation of such infrastructure, linking this unsettled issue to capacity-building and calling for closer interstate and public-private cooperation.

The 2021 GGE report develops means of compliance with the voluntary, non-binding norms of responsible state behavior agreed upon in 2015. Like the OEWG, it stresses the importance of international cooperation, the value of CBMs, and capacity building. Although regional organizations like the OSCE are strong drivers in the development and implementation of CBMs, the major powers that participated in both UN sponsored groups expressed conflicting views about such regional level activity. Some feared a duplication of efforts, while others raised questions about the financing of such capacity building measures.

Overall, the GGE reemerged as the main inclusive process on the application of international law to cyberspace and demonstrated significant progress from its previous rounds, although a number of issues still deserve close attention. Issues such as sovereignty, due diligence, interreference, the meaning of "attack" in the cyber realm, the scope of state accountability, and countermeasures remains unsettled, as do calls for a transparent mechanism to assess and track the progress of norm implementation. Perhaps the greatest value of the GGE's report is the progress made in recognizing the application of IHL to cyberspace and in the norm around the value and effects of attribution. Clear added value is also provided by the report's practical advice and guidance on norm implementation.

Conclusion

Although none of the parallel UN processes resulted in groundbreaking agreements on application of international law to cyberspace and mainly display very cautious language, by encouraging dialogue on critical issues, as well as public state declarations on national approaches and interpretations of international law, these deliberations themselves represent confidence-building measures.

While establishing concrete regulations for cyberspace is not a speedy process and fragmentation on fundamental issues cannot be ignored, the sophistication of destructive cyber capabilities has dramatically increased. Both the OEWG and GGE reports were long-expected, but how these two parallel diplomatic negotiations influence each other—or can be reconciled in the future—is hard to predict. An important endeavor would be to clearly determine the future rules of the road, whether that entails the planning of a multilateral binding instrument or further elaboration of voluntary non-binding rules. Both reports tend to point towards the latter approach, but it would be useful to assess whether the priority now should be the development of additional voluntary non-binding norms or the implementation of existing ones. The overlapping mandate of these two working groups and the duplication of efforts in parallel fora certainly complicates reaching common ground.

About the Author: Adina Ponta is currently a teaching lecturer at the Babeș-Bolyai University in Romania, and a postdoctoral researcher at the Law School' s Center for Business Law & Information Technology. She was the 2020 Detlev F. Vagts International Law Fellow at the American Society of International Law. Prior to that, she spent four years in the legal offices of two NATO headquarters, where she advised on the lawful conduct of armed forces during conflict and peacetime military operations. Her professional experience includes assignments in the German Parliament, United Nations, embassies, and in academia. She has an LL.M. in international law and a Ph.D. in business and technology law.

[1] UN GA A/RES/73/266, https://undocs.org/A/RES/73/266; UN GA A/RES/73/27, https://undocs.org/A/RES/73/27.

[2] UN GA A/RES/75/240, https://undocs.org/en/A/RES/75/240.

[3] Final OEWG Report https://www.un.org/disarmament/open-ended-working-group/.

[4] ICRC position paper to the OEWG (2019), https://unoda-web.s3.amazonaws.com/wp-content/uploads/2020/01/icrc_ihl-and-cyber-operations-during-armed-conflicts.pdf.

[5] Patryk Pawlak, *Confidence-Building Measures in Cyberspace: Current Debates and Trends,* Legal, Policy & Industry Perspectives, Anna-Maria Osula and Henry Rõigas (eds.) (2016).

[6] Report of the GGE on Advancing responsible State behaviour in cyberspace in the context of international security, https://front.un-arm.org/wp-content/uploads/2021/06/final-report-2019-2021-gge-1-advance-copy.pdf.