Norms vs. Realities: Cyber at the UN

In the wake of Russia's invasion of Ukraine, cyber norms discussions at the UN have reached an impasse. Tensions between the US and Russia have stalled substantive progress, particularly on issues of cyber conduct during armed conflict. Yet, the continued existence of the UN working groups is a small but positive sign for the future, as is the growth of norm discussion venues beyond the UN.

By Taylor Grossman

Portrait of a UN flag on a computer motherboard, October 2022. *Designed by Kevin Kohler and generated using DALL-E OpenAI*

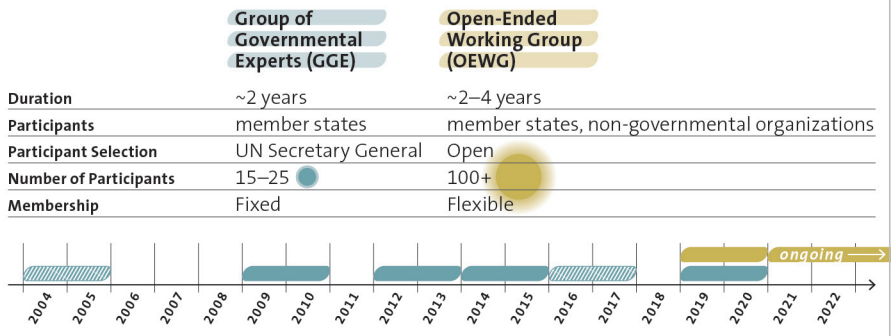
Amidst the global expansion of information communications technologies (ICT) in the 1980s and 90s, governments faced new and fundamental regulatory questions: How should they handle this domain in terms of national defense, state sovereignty, criminal activity, and other core state prerogatives? In these early years, no agreements yet existed on how to apply international law to cyberspace. Many early Internet pioneers eschewed state interference. In Switzerland in 1996, cyber libertarian John Perry Barlow outlined a declaration of independence for cyberspace. Others began to wonder whether cyberspace would need an entirely new set of norms of behavior (See CSS Cyberdefense Report: One, Two, or Two Hundred Internets?).

Against this backdrop of uncertainty, the UN came to serve as an important focal point for cyber norm development. Over the past two decades, the UN has helped frame ICT within the lens of existing international norms and law, including its founding charter, and has established a degree of continuity of responsible state behavior across domains, folding cyberspace into the laws that govern state interaction at sea, on land, and in the air. In particular, the UN has sought to find minimum common norms to reduce the risk that cyberspace becomes a source of instability, escalation, and harm – particularly to civilians. Switzerland has been central to these efforts, from its commitment to Geneva as the "capital of digital governance," to its role as a chair of previous rounds of UN norms discussions, to its interest in neutrality in cyberspace (See CSS Cyberdefense Report: The Law of Neutrality in Cyberspace).

Yet despite this ambitious premise, the two resulting UN-led processes – the six Groups of Governmental Experts (GGEs) convened between 2004 and 2021, and the two Open-Ended Working Groups (OEWGs) since 2019 – have led to modest, stilted results. Major powers like Russia, China, and the US have generally shied away from specificity in cyber norm articulation. While China has sometimes worked with other state delegations to advance its viewpoints, Russia has been central to both

UN processes – albeit often in the role of spoiler. Thus far, states have agreed to the general applicability of international law to cyberspace, but most governments have yet to advance positions on specific legal issues. In the case of international humanitarian law (IHL) – also known as the law of armed conflict – there is even less consensus. Beyond a broad allusion to its potential relevance in the GGE consensus report of 2021, UN discussions have been unable to develop further practical understandings. Non-state actors, meanwhile, have sought a greater voice in norms discourse and have frequently advocated for more robust normative restraints on state behavior.

UN Norms Processes at a Glance



Sources: Adapted from Reaching Critical Will and DigiWatch

Russia's war in Ukraine has exacerbated already fragile UN consensus-based fora for norms discussions, as demonstrated in recent procedural and substantive roadblocks at the latest round of working group meetings in New York. The spring and summer OEWG meetings on security of and in the use of ICT were substantive in name only: the working group did manage to produce a consensus progress report, albeit one with almost no concrete advancements. This generally lackluster performance underscores a growing divorce between norms discussions and the realities of interstate politics, as these platforms have done very little to address the ongoing situation in Ukraine. Ultimately, the most important aspect of the working group is its continued existence as a touchpoint for engagement and as encouragement for other avenues of norm implementation. Switzerland has continued to advocate for a robust UN-based process and has also helped to expand the roster of working group participants, leading to a promising rise in norm implementation venues beyond the United Nations.

A Tale of Two Processes

In 1998, the Russian delegation to the UN proposed a provisional agenda item on ICT, citing the potential adverse effects these new technologies could pose to both international stability and state security. The UN First Committee on Disarmament and International Security eventually created a GGE to examine the issue, a now popular mechanism for exploring new fields by providing a concrete platform for convening subject matter experts to deliberate and recommend actions without tying states to binding resolutions. Six Groups of Governmental Experts (GGEs) were eventually convened between 2004 and 2021, with mixed success. While the first GGE failed to produce a consensus report, later GGEs were able to take tentative steps forward. Most importantly, the 2013 GGE report affirmed the applicability of international law to state use of ICT, and the 2015 report outlined a set of eleven voluntary norms of state behavior. These GGEs have had narrow mandates: the focus has been on political and military issues, rather than on technical aspects of cyber-related technologies. For example, the 2015 report suggests a norm that states restrain from targeting each other's critical infrastructure, rather than including specific provisions limiting technical methods or exploits that might be used against critical infrastructure.

> There is a growing divorce between norms discussions and the realities of interstate politics.

After these seeming breakthroughs, however, the GGE process began to devolve. Faced with increasingly difficult questions about how to apply the voluntary norms it had set out two years earlier, the 2017 GGE was unable to produce a consensus report. Russia, meanwhile, moved to create a separate venue for cyber norm discussion through a new Open-Ended Working Group (OEWG). The OEWG was ostensibly established to enable more robust and equitable participation. Yet despite its purported advantages, Russia's push for a new forum within the UN was more likely an attempt to complicate and derail an already delicate process. Many states worried that the OEWG would create competing, contradictory normative frameworks, further diluting the effects of non-binding GGE reports.

The GGE process is bounded: the Secretary General selects participants at the outset, and membership is capped to a small number (15–25) of state representatives. Membership is also fixed for the duration of each GGE. The OEWG, by contrast, can easily become unwieldy as it includes all 193 member states. Participants do not have to attend each meeting but can contribute where they see fit over the course of the working group. The OEWG is also open to non-governmental organizations (NGOs): civil society groups, academia, and industry can petition to join and provide feedback throughout the process. Accredited groups can attend OEWG meetings as observers and engage in informal consultancies throughout the process.

Russia's interest in promoting state sovereignty and internal security has been increasingly at odds with the broader movement of the GGEs towards international restriction of state activities in cyberspace. Russia's focus on internal security has been clear from the very outset of its 1998 proposal, and subsequent statements have emphasized "information security," which includes "political and ideological" threats emanating from cyberspace, over "cybersecurity," which it sees as narrowly technical. Practically, information security encompasses issues of content moderation and restriction, allowing for more explicit government intervention in information access to ensure domestic stability. UN norms processes have generally used blander terms such as "ICT security" to try and

sidestep the issue, but the underlying tensions between a more open cyberspace and one that is amenable to increased government intervention continue to frustrate progress in New York and Geneva.

Recent Evolutions

Despite initial concerns over the two-track process within the UN, 2021 ended up being a year of surprising success for cyber norms. The Sixth GGE concluded with a consensus report, including a cautious step forward on IHL and its potential applicability in state ICT use. Switzerland has been a key advocate for the expansion of IHL to cyber activities, releasing a position paper in conjunction with the GGE report that went beyond its findings to assert that IHL is the primary body of law governing cyber operations in an armed conflict. The first OEWG, which had been chaired by Ambassador Jürg Lauber of Switzerland, also produced a consensus report which endorsed the conclusions of earlier GGEs and further reaffirmed the importance of UN-led discussions on cyber technology in the context of international security. Ambassador Lauber also led the way in soliciting participation from smaller regional organizations, expanding the OEWG to include a broader array of expertise. A second OEWG was stood up in December 2021, to conclude in 2025.

Russia and the US also took steps to strengthen their diplomatic engagement in cyberspace. In June 2021, American President Joe Biden and Russian President Vladimir Putin met in Geneva to discuss ways to reduce tensions and curtail cyberattacks against their respective countries. In the following months, the number of cyberattacks seemed to subside somewhat, and both the US and Russia entered a new and tentative working relationship to crack down on malicious hackers operating within their borders. In October, Russia and the US submitted a joint proposal to the UN General Assembly First Committee that underscored both countries' commitment to the OEWG and GGE processes and the resulting consensus reports. Fifty countries co-sponsored the resolution, and it was adopted without a vote in the beginning of November.

Almost a year later, such a resolution seems like a relic of a bygone era. Russia's invasion of Ukraine in February 2022 caused major disruptions in international diplomacy that have inevitably reverberated across the realm of cyber norms. Strained relations between the US and Russia have made progress on the November resolution all but impossible and have raised the temperature at the ongoing OEWG. The cyber domain has played a key supporting role on the battlefields of Ukraine, including in Russia's early move to conquer Kyiv and in the novel approach of the IT Army of Ukraine. In the days preceding the February invasion, Russia launched a supply chain attack that disrupted satellite communications across the country. The Kremlin has also been behind a variety of distributed denial of service (DDoS) and data destruction campaigns levied against the Ukrainian government and people. The IT Army of Ukraine, meanwhile, has authored coordinated campaigns defacing and overloading Russian web services usually through DDoS attacks. Although the strategic value of these incidents is still unclear, the IT Army has openly recruited participants from outside Ukraine, including in EU and NATO member states (See CSS Cyberdefense Report: The IT Army of Ukraine). These developments test the conclusions of past consensus reports, raising significant questions about due diligence obligations, critical infrastructure protection, and participant classification in cyberspace.

Breakdown at the OEWG

Yet, the UN seems poorly positioned to make any progress on addressing the realities of the conflict through its norm discourse. Instead, the OEWG has been plagued by procedural squabbling and subject-matter gridlock. Participation became particularly politicized when 32 civil society organizations were rejected from joining the July sessions in New York. Russia was behind most of the denials. Although the country gave no public explanation for its decisions, the groups barred from participation generally had western credentials. Ukraine rejected a small number of groups as well, asserting that the organizations were too closely linked to the Russian state to be true non-governmental participants.

> Governments are not monoliths in cyberspace: the majority of global ICT is privately owned and operated, and critical infrastructure is increasingly outside the hands of the state.

The rejection of NGOs in June betrays a defining advantage of the OEWG process, which is its openness. The working group setup allows for a more flexible and inclusive array of actors to join in the norms debate. Governments are not monoliths in cyberspace. The majority of global ICT is privately owned and operated, and critical infrastructure is increasingly outside the hands of the state. NGOs already play a key role in the de facto governance of cyberspace, from the civil society organizations who provide significant expertise and capacity on incident response and remediation, to the multinational companies that run much of the Internet. The exclusion of these groups from norm setting and implementation is shortsighted, as organizations like the Cyber Tech Accords (a consortium that represents major American and European private sector interests in ICT) and FIRST (a network of global computer incident responders) will continue to play substantial roles in cyberspace, regardless of their presence at the New York meetings.

Substantive Stalemate

Perhaps as expected, the OEWG took even fewer steps toward resolving subject matter disputes. Even in the realm of confidence-building measures – activities and processes that are instituted to reduce tension or mistrust between states, thereby limiting the potential for escalation and conflict – the OEWG found itself at an impasse. A cyber crisis hotline, reminiscent of the famous nuclear crisis hotline established between Moscow and Washington during the Cold War, had been proposed in earlier meetings. Yet, the OEWG has been unable to move forward on a specific implementation plan. Even a recommendation to strengthen computer emergency response team cooperation was removed from the final progress report. If the OEWG cannot make progress on such seemingly non-controversial areas, where can it hope to find common ground?

Further Reading

Duncan Hollis, **"A Brief Primer on International Law and Cyberspace,"** *Carnegie Endowment for International Peace,* 14.06.2021.

Camino Kavanagh, **"Ukraine: Cyber Operations and Digital Technologies,"** *Directions Blog,* 22.03.2022..

Louise Marie Hurel, **"The Rocky Road to Cyber Norms at the United Nations,"** *Council on Foreign Relations,* 06.09.2022.

The OEWG also stumbled on the issue of IHL and its applicability in cyberspace. Particularly in the context of Russia's war in Ukraine, IHL has become a major point of contention. Past GGEs and the present OEWG have been unable to move beyond the vaguest allusions to basic IHL principles, such as indications that proportionality and distinction may be relevant in cyberspace. When it comes to specific applications, consensus reports have been noticeably silent. Regardless of this standoff, however, cyber operations are finding their place on the battlefield. IHL principles are clearly at issue here, and questions surrounding who constitutes a combatant and what kinds of actions are proportional will eventually rise to other international legal arenas. Yet, in today's climate, progress on these questions seems both more urgent and more improbable.

UN multilateral fora remain important touchstones for debate, particularly as other diplomatic avenues have broken down over the past year.

Outlook

OEWG stagnation is evidence of a further fracturing geopolitical environment, as tensions mount between Russia and the West. Despite its limited progress this year, however, many members of the group have pointed towards its very existence as a confidence-building measure. UN multilateral fora remain important touchstones for debate, particularly as other diplomatic avenues have broken down over the past year. Indeed, that Russia, Ukraine, the US, and the EU even met in New York to discuss cyber norms in March and July of this year seems like a minor miracle. For Switzerland, the continuation of UN norms discourse is a sign that many states have an abiding interest in a stable, governable cyberspace.

While in the short- to medium-term, the prospects for major advancements are not promising, Switzerland has a clear stake in a credible and open UN process. Switzerland promoted meaningful inclusion of NGOs in the UN process, and thanks in part to Swiss advocacy efforts, the OEWG has also led to a proliferation of norms discussions in regional and non-governmental venues that will hopefully yield more fruitful results. This profusion of smaller settings for norms deliberation is a welcome signal that while the West and Russia may be in a prolonged standoff, other countries are trying to take incremental steps forward.

For more on perspectives on Cyber Security Politics, see CSS core theme page.

Taylor Grossman is Senior Researcher in the Cyberdefense Project with the Risk and Resilience Team at the Center for Security Studies (CSS) at ETH Zürich.

CSS Analyses in Security Policy is published by the Center for Security Studies (CSS) at ETH Zürich. The CSS is a center of competence for Swiss and international security policy. Each month, two analyses are published in German, French, and English.

Editor: Névine Schepers
Language Editing: Névine Schepers
Layout and graphics: Miriam Dahinden-Ganzoni

Feedback and comments: analysen@sipo.gess.ethz.ch
More editions and online subscription: www.css.ethz.ch/cssanalyses

ISSN: 2296-0244; DOI: 10.3929/ethz-b-000577969