Cyberstability Paper Series

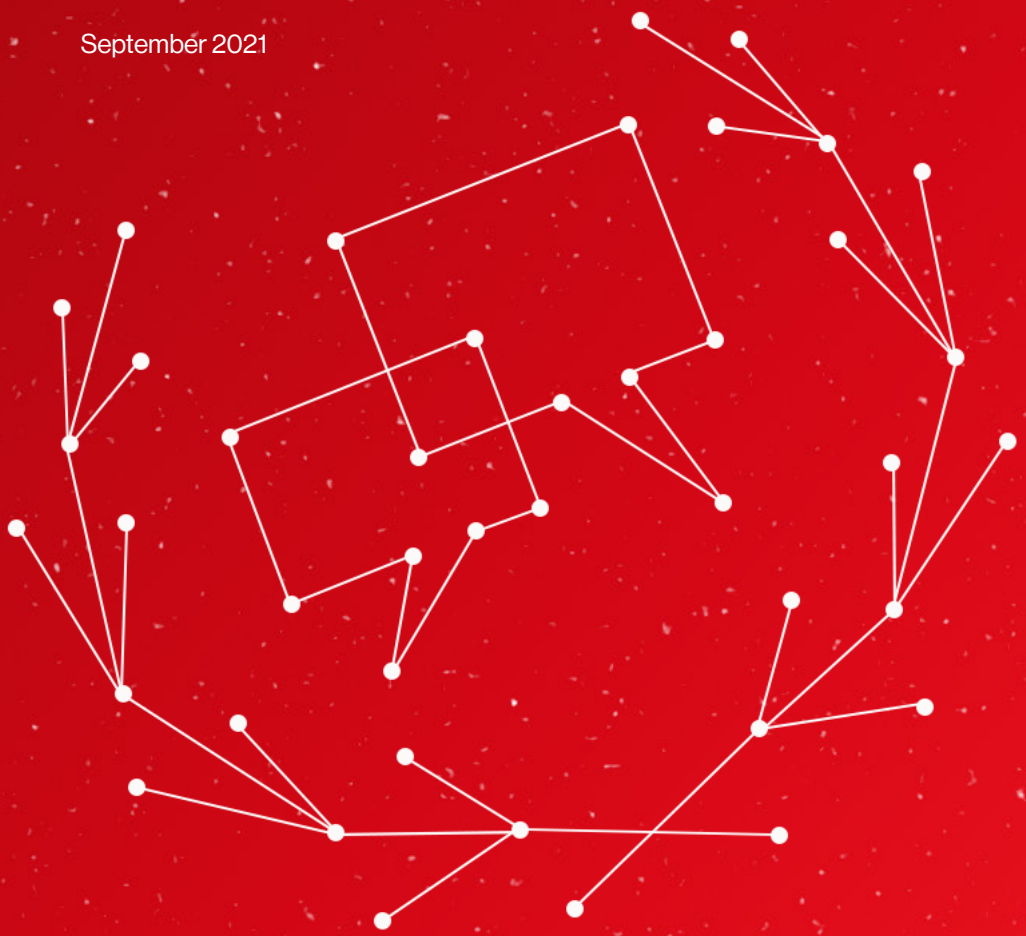
New Conditions and Constellations in Cyber

From Confrontation to Consensus: Taking Stock of the OEWG Process

Ambassador Jürg Lauber
Chair of the first UN Open-ended Working Group on developments in the field of information and telecommunications in the context of international security from 2019 until 2021.

Lukas Eberli
Second Secretary for Cybersecurity at the Permanent Mission of Switzerland to the United Nations and other international organizations in Geneva

September 2021



Cyberstability Paper Series
New Conditions and Constellations in Cyber

From Confrontation to Consensus: Taking Stock of the OEWG Process

Ambassador Jürg Lauber | Chair of the first UN Open-ended Working Group on developments in the field of information and telecommunications in the context of international security from 2019 until 2021.

Lukas Eberli | Second Secretary for Cybersecurity at the Permanent Mission of Switzerland to the United Nations and other international organizations in Geneva

September 2021

On 28 April 2021, the General Assembly of the United Nations ("UNGA") endorsed[1] the report of the Open-ended Working Group on developments in the field of information and telecommunications in the context of international security ("OEWG"). The UNGA's decision brought to a close a process that had been initiated by the General Assembly's First Committee in the fall of 2018, and whose successful outcome came as a surprise to many. The OEWG report provides a very strong reconfirmation of the existing normative framework with regard to cybersecurity, while it adds a number of essential new elements and offers a rich compendium of ideas and proposals for future deliberations on the same issue. The first-ever UN Open-ended Working Group on this issue brought cybersecurity into the multilateral mainstream, with the UN General Assembly at its center. It made a strong case for universal participation in discussions of a topic that is vital to all nations.

I had the privilege of serving as the Chair of this first OEWG. In this article, I will mainly describe the OEWG process from the Chair's perspective and try to explain how and why we were able to pull back from confrontation and reestablish consensus. I will also give a brief and personal assessment of the outcome and, finally, share a few thoughts about the way forward.

Ambassador Jürg Lauber currently serves as the Permanent Representative of Switzerland to the United Nations Office and the other international organizations in Geneva. He served as the Chair of the first UN Open-ended Working Group on developments in the field of information and telecommunications in the context of international security from 2019 until 2021.

Lukas Eberli served as the Adviser to Ambassador Jürg Lauber's Chairmanship of the UN OEWG. Currently, he Second Secretary for Cybersecurity at the Permanent Mission of Switzerland to the United Nations and the other international organisations in Geneva.

When the General Assembly of the United Nations established the OEWG in December 2018 by Resolution 73/27[2], this particular format—enabling the participation of all Member States and observers of the United Nations—was a first for cybersecurity. The issue, however, was far from new to the United Nations. It had been on the agenda since 1998 and was primarily dealt with by five subsequent Groups of Governmental Experts on Advancing responsible State behavior in cyberspace in the context of international security ("GGE"). In addition, there had been annual reports by the Secretary-General to the General Assembly with the views submitted by UN Member States on the issue. By 2015, the GGE format had produced a sophisticated normative framework (often referred to as the "acquis"), essentially comprising three pillars: 1) Eleven non-binding norms of responsible state behavior in cyberspace, 2) A common understanding of the applicability of existing international law, and 3) Confidence-building measures. No progress was achieved in the following years, and the inability of UN Member States to find consensus in their deliberations on the subject of cybersecurity was starting to threaten the integrity of the 2015 acquis. Indeed, the Russian draft resolution to establish the OEWG was opposed by a significant number of delegations[3] for its particular interpretation of earlier agreed-upon voluntary non-binding norms.

According to its mandate as contained in Operational Paragraph 5 of UNGA Res 73/27, the OEWG was to deliberate and report on six items:

- First, Existing and Potential Threats;
- Second, Rules, Norms and Principles;
- Third, International Law;
- Fourth, Confidence-Building Measures;
- Fifth, Capacity-building; and
- Sixth, Regular Institutional Dialogue.

Importantly, the OEWG was required to adopt its report by consensus. Finally, the mandate offered a first, if cautious, opening toward non-governmental stakeholders ("namely, business, non-governmental organizations, and academia"; hereafter generally referred to as "stakeholders").

Based on draft resolution 73/266 of 22 December 2018[4], submitted by the United States, the General Assembly of the United Nations also established another, sixth GGE with a very similar mandate and twenty-five members. This led to the unusual situation of having two UN bodies dealing in parallel with almost the exact same issues.

For the OEWG Chair, the central task was to work with the Group in such a way as to soften the fronts that had hardened since 2015, and ultimately present a document that would be acceptable to all States as well as deliver added value for as many as possible. The GGEs of the past had comprised up to twenty-five members. In the OEWG, all 193 Member States of the United Nations would have a say. The much higher number and diversity of the OEWG made the challenge to find consensus all the more daunting, but it also offered the promise of new dynamics emanating from groups and individual Member States that had little or no representation in previous GGEs. This is, e.g., reflected in the very substantive chapter on cybersecurity capacity-building in the OEWG's report, an issue that had never attracted this much attention in past GGEs. With this in mind, I based my strategy for the negotiation process on the principles of inclusiveness, transparency, and cautious ambition. For instance, my team and I made great efforts to reach out to the various regional and other groups of Member States as well as to the so-called (non-governmental) stakeholders. We wanted to ensure that as many of them as possible would participate in the deliberations, thus underpinning the legitimacy of the process and its possible outcome. We also made sure that all

interested parties had equal access to information about the Chair's intentions with regard to the process and the draft report.

According to the mandate of the OEWG and the original work plan, we had scheduled three substantive sessions, one intersessional stakeholder meeting, and two informal intersessional meetings, between September 2019 and July 2020. Things were looking very good at the end of the second substantive session in February 2020. By that time, we had seen an exceptionally high level of participation from UN Member States and observers, as well as the buildup of a very positive dynamic among delegates. It had paid off to focus on issue presentations and discussions rather than on negotiations. When the OEWG began its work, the majority of delegations had never seriously engaged with cybersecurity in a UN context. It was important to give them the opportunity to familiarize themselves with the subject and its history in previous UN processes. I want to mention in particular, among the fresh voices that brought new energy to the deliberations on cybersecurity at the UN, the group of young female diplomats from various regions of the world, whose participation was encouraged and facilitated by the Women in International Security and Cyberspace Fellowship[5].

When the OEWG began its work, the majority of delegations had never seriously engaged with cybersecurity in a UN context.

Only a few days after the second substantive session, the disruptive force of the COVID-19 pandemic became all too obvious. Over the following months, we had to adapt the OEWG work plan several times. From traditional physical meetings we switched first to consultations by correspondence and then to a virtual format. Instead of July 2020, the third and final substantive session was held in March 2021 in a peculiar virtual/hybrid format. Fortunately, the mutual trust and overall positive momentum we were able to build prior to the pandemic did not dissipate during the period of virtual meetings, but carried us all to a successful conclusion of our mandate.

Aside from the impact of COVID-19, there were additional factors that complicated the process. The fact that the resolution establishing the OEWG was controversial and had to be voted on was obviously less than ideal. It was also a reflection of the current geopolitical environment, which is not exactly conducive to consensus on a global level. Furthermore, the new open-ended format, while offering the promise of new ideas and dynamics, required special efforts to create a reasonably level playing field for delegations.

There were also many elements that contributed positively to the process. The very high turnout was a strong indication of the rapidly growing awareness of cybersecurity threats, which has been exacerbated by the rapidly increasing number of cyberattacks on healthcare and scientific institutions since the COVID-19 pandemic outbreak. This certainly reinforced the general sense among delegations that progress needs to be made. More specifically, several delegations and individual delegates went above and beyond to contribute to the Group's success. The numerous proposals on the Group's website[6] are testament to this. Finally, the positive outcome would have been impossible without the technical expertise, institutional memory, and high availability of the UN support team (UNODA, UNIDIR, UNDGACM) under the leadership of the UN High Representative for Disarmament Affairs, Under-Secretary-General Izumi Nakamitsu.

The concurrent activities of the first OEWG and the sixth GGE did *not* prove to be a complicating factor, as some delegations had feared at the outset. The very different composition of the groups made for equally different approaches and working methods. In addition, the excellent relationship between the chair of the GGE, Ambassador Guilherme Patriota of Brazil, and myself was very help-

ful in avoiding any competition or contradictions between the two bodies. It is also noteworthy that the delegations who had voted against one resolution or the other in establishing the two groups nevertheless fully engaged once the work started. Ultimately, the processes and outcomes of the two groups were nothing but complementary and mutually reinforcing.

The OEWG concluded its work with a two-part report. The Final Substantive Report[7] contains those elements on which the delegations achieved consensus. Most importantly, it reestablished consensus on the 2015 acquis and it did so in a particularly meaningful way. In the past, the GGE reports had been agreed upon among the members of the Group and subsequently adopted by the General Assembly of the United Nations as a simple formality. In reality, beyond the members of the GGE, only a few delegations showed serious interest in the GGE's work or their reports. Meanwhile, with the OEWG, every Member State was offered the opportunity to contribute throughout the process and none would be able to pretend ignorance of its outcome. In this way, the OEWG has reaffirmed and significantly strengthened the existing normative framework. Beyond that, the Final Substantive Report contains various new elements that update and expand the acquis, of which I want to mention just a few examples.

The report provides a step forward in the Member States' assessment of the cyber threat landscape, as it mentions attacks on medical facilities and the need for their protection, also under the existing agreed-upon norms, as well as the impact of cyberattacks on healthcare infrastructure in the context of the COVID-19 pandemic. It recognizes the devastating humanitarian consequences of cyberattacks, and mentions practical measures as first steps toward building confidence, such as the designation of a national Point of Contact. Furthermore, the report recognizes the need for the protection of critical information infrastructures, including the need to ensure the general availability and integrity of the internet, often referred to as the public core of the internet. The strongest section of the report deals with capacity-building, in which it underscores the need for building cybersecurity capacity, pointing out that cybersecurity capacity-building is a two-way street, and offering a list of principles as guidance for capacity-building. The report also underscores the importance of narrowing the "digital divide," including the "gender digital divide," and pays tribute to the role of (non-governmental) stakeholders. In its last chapter, it recognizes the need for a regular, institutionalized forum for dialogue among States on the use of ICTs in the context of international security.

With the OEWG, every Member State was offered the opportunity to contribute throughout the process and none would be able to pretend ignorance of its outcome.

The Chair's Summary[8] contains those elements on which the delegations did not (yet) achieve consensus. It offers several orientations as well as a vast compendium of ideas and proposals that will encourage and enrich future discussions of cybersecurity. To name only a few, the collection of proposals for new norms, as well as the proposed guidance on the implementation of existing norms, will hopefully inspire future discussions. Readers may want to take a closer look at the actual document on the Group's website.

In addition to its actual outcome, the OEWG succeeded through its negotiation process in attracting attention and providing important impetus for accelerated engagement with the issue of cybersecurity by governmental and nongovernmental actors at the international, regional, and national levels.

Also, the above-mentioned inclusiveness of the OEWG went beyond the Member States and observers of the United Nations and opened a new chapter of stakeholder participation in an in-

tergovernmental process on cybersecurity. While there is still room for improvement, non-state stakeholders played a much bigger role than in the past. Their presence and contribution were particularly strong during the Informal intersessional consultative meeting with Industry Partners and NGOs, which was held from 2 to 4 December 2019 in New York. Upon my request, the meeting was chaired by David Koh, Chief Executive of the Cyber Security Agency of Singapore, who submitted a separate Chair's Summary[9] that is annexed to the two-part OEWG report. Furthermore, the many written contributions by representatives of academia, non-governmental organizations, and the private sector from across the globe can be found on the Group's website. These contributions, as well as the numerous formal and informal formats of exchange with Member States, enriched the discussions of the OEWG and allowed for a more inclusive result, which is reflected among other elements in the references to a human-centric approach in cybersecurity and the importance of narrowing the gender digital divide.

OEWG went beyond the Member States and observers of the United Nations and opened a new chapter of stakeholder participation in an intergovernmental process on cybersecurity.

The successful conclusion of the OEWG came as a surprise to many and was generally welcomed with great relief and considerable satisfaction. However, as is usual in this type of exercise, hardly any delegation would declare—or openly admit—that they are completely satisfied with the result. Indeed, nobody got all their wishes. As Chair, I would have liked to have seen language in the report that was less prone to "UN speak" and better suited for public consumption. As Switzerland, we would have preferred an even stronger reference to the applicability of International Humanitarian Law. Pick any delegation and they will identify one or several shortcomings of the two-part report. In the end, none of the shortcomings seemed important enough to derail the process.

Herein lies one of the lessons we learned from the OEWG process: Multilateralism works! The delegations recognized the importance and urgency of addressing the issues relating to cybersecurity at a global level. After months of emphatic arguments and tough negotiations, they settled for compromise, because they knew that consensus was not a zero-sum game.

Meanwhile, the limits of that upon which Member States are currently willing to agree also became clear. Many fundamental differences persist, not all of which are exclusive to cybersecurity. One important difference pertains to the role of the international normative framework. Is the current framework sufficient for ICTs or does it require modifications or amendments? Should new norms be aspirational or immediately binding? In case of the latter, should their implementation be monitored by an international body, and should violations be sanctioned?

The OEWG process also offered a few early lessons in virtual diplomacy. As described above, the Group had a steep learning curve in the use of virtual conferencing platforms. In spite of several obstacles well known by anybody who may have recently been involved in international video-conferencing, the Group quickly adapted to the new tools, and the high participation and positive dynamic prevailed to the end. However, it is difficult to imagine this outcome if we had not had sufficient time before the outbreak of the pandemic to establish the necessary personal relationships and trust between delegates and between delegates and the Chair.

The discussion around cybersecurity has, fortunately, not stopped with the conclusion of the OEWG. Only a few weeks later, the GGE successfully finished its work, adding additional elements that will strengthen the normative framework for cybersecurity. In December 2020, the General

Assembly had already decided to establish a second OEWG, with a very similar mandate and a timeframe from 2021 to 2025. On 1 June 2021, the new OEWG held its organizational session and elected my former colleague, Ambassador Burhan Gafoor, the Permanent Representative of Singapore to the United Nations, as its Chair. In discussions during the first OEWG, many delegations expressed their hope that we would return to a single multilateral process on cybersecurity at the UN level. The new OEWG is likely to be able to play this role, as long as it is able to accommodate new ideas and proposals, such as the "Programme of Action," originally suggested by Egypt and France and now supported by many States from around the world. Also, the new OEWG needs to avoid being perceived as merely a "talk shop," but must deliver results well before its five-year mandate expires.

In addition to the work at the UN level, discussions and efforts to contain cybersecurity threats on regional and national levels are to be welcomed and supported. Such initiatives may deliver progress more quickly, and they are likely to offer valuable lessons for other regions or on a global scale. In this context, it was interesting to see that cybersecurity was one of the priority items on the agenda of the recent summit meeting between presidents Joe Biden of the United States and Vladimir Putin of Russia, which took place in Geneva, Switzerland. There is little doubt that any progress in their bilateral discussions on this topic would create a positive impetus to negotiations at the United Nations.

In any intergovernmental discussions on cybersecurity, be they on the international or regional level, States would have much to gain from better inclusion of stakeholders, such as the private sector, academia, and civil society. The area of international security and peace is particularly sensitive and remains by and large a core responsibility of states. Meanwhile, there is no denying that non-state actors play an important role, especially when it comes to cybersecurity, and that stakeholders have much to offer in terms of expertise and possible solutions. The above-mentioned Informal intersessional consultative meeting with Industry Partners and NGOs is an excellent example and proved to be a very fruitful encounter between (non-governmental) stakeholders and Member States. Much of its success is due to the excellent preparation of the event by the United Nations Office for Disarmament Affairs.

As much as the recent successes of the OEWG and the GGE are to be welcomed, the reality as reported in the media on an almost daily basis offers a bleaker picture. While diplomats succeeded in strengthening the international normative framework to promote responsible state behavior in cyberspace, the number and severity of violations of said framework by states and others seem to go up rather than down. The threat of escalation from "cyber incident" to open cyber conflict and beyond is rapidly increasing. Sooner rather than later, states will have to address issues such as attribution, accountability, and sanctions. Failure to do so may end up weakening the normative framework, as norms that are repeatedly violated with impunity carry little respect. In the meantime, efforts to strengthen confidence-building measures and capacity-building are more likely to succeed in the short term. Investments in the latter are urgently needed and likely to make a significant contribution to better prevention against malicious use of ICTs. All in all, the agenda of the OEWG seems just as relevant for future deliberations on developments in the field of information and telecommunications in the context of international security. The work never stops.

In any intergovernmental discussions on cybersecurity, be they on the international or regional level, States would have much to gain from better inclusion of stakeholders, such as the private sector, academia, and civil society.

Endnotes

1 United Nations General Assembly (75th session: 2020-2021). "Report of the Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security established pursuant to General Assembly resolution 73/27 of 5 December 2018". United Nations Digital Library, 2021. https://digitallibrary.un.org/record/3924426?ln=en.

2 United Nations General Assembly (73rd session). "Developments in the field of information and telecommunications in the context of international security". United Nations, December 5, 2018. https://undocs.org/en/A/RES/73/27.

3 The Resolution was eventually adopted in the UN General Assembly by 119 against 46 votes and 14 abstentions (among them Switzerland).

4 United Nations General Assembly (73rd session). "Advancing responsible State behaviour in cyberspace in the context of international security". United Nations, December 22, 2018. https://undocs.org/en/A/RES/73/266.

5 Please see: https://cybilportal.org/projects/women-and-international-security-in-cyberspace-fellowship/.

6 United Nations Office for Disarmament Affairs. "Open-ended Working Group". United Nations. https://www.un.org/disarmament/open-ended-working-group/.

7 United Nations General Assembly. "Open-ended working group on developments in the field of information telecommunications in the context of international security. Final Substantive Report". United Nations, March 10, 2021. https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf.

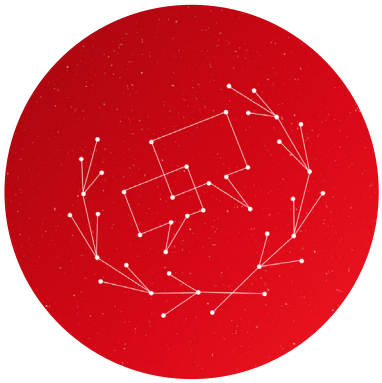
8 United Nations General Assembly. "Open-ended working group on Developments in the Field of Information and Telecommunications in the Context of International Security. Chair's Summary". United Nations, March 10, 2021. https://front.un-arm.org/wp-content/uploads/2021/03/Chairs-Summary-A-AC.290-2021-CRP.3-technical-reissue.pdf.

9 Let's Talk Cyber. "Informal Multi-Stakeholder Cyber Dialogue. Summary Report". United Nations, December 04-10, 2020. https://front.un-arm.org/wp-content/uploads/2020/12/informal-ms-dialogue-series-summary-report-final.pdf.

About the Authors

Ambassador Jürg Lauber currently serves as the Permanent Representative of Switzerland to the United Nations Office and the other international organizations in Geneva. From 2015 to 2020, he served as Permanent Representative of Switzerland to the United Nations in New York. In parallel, he served as the Chair of the first UN Open-ended Working Group on developments in the field of information and telecommunications in the context of international security from 2019 until 2021. As a diplomat, he was previously posted in Bangkok, Bern, Beijing, Geneva, and New York. Between 2007 and 2009 he served as chef de cabinet to the President of the International Criminal Court. Before joining the Swiss Federal Department of Foreign Affairs in 1993, he worked in peacekeeping missions in Namibia (UNTAG) and Korea (Panmunjom).

Lukas Eberli served as the Adviser to Ambassador Jürg Lauber's Chairmanship of the UN OEWG from 2019 to 2021. He is currently holding the position as Second Secretary for Cybersecurity at the Permanent Mission of Switzerland to the United Nations and the other international organisations in Geneva. From 2019 until 2020 he was working at the Permanent Representation of Switzerland to the United Nations in New York, first covering Security Council issues and later Cybersecurity and Digital Cooperation. Lukas Eberli joined the Swiss Federal Department for Foreign Affairs in 2018, working at the Embassy of Switzerland in Jakarta, Indonesia. Before joining the Department, he worked as a political consultant for Members of the Swiss Federal Parliament.



About the Cyberstability Paper Series

Since the release of the final report of the Global Commission on the Stability of Cyberspace in November 2019, the concept of cyberstability has continued to evolve. A number of new 'conditions' are emerging: new agreements on norms, capacity building and other stability measures have been proposed and solidified within the United Nations and elsewhere, and stakeholders are exploring ways to increase stability and minimize the risk of conflict in cyberspace through technical fixes or governance structures. The constellations of initiatives involved in working towards cyberstability is expanding, underlining the need to connect the traditional state-led dialogues with those of the Internet communities from civil society and industry. Gaps continue to close, between the global north and south, between technology and policy, but also the stability in and the stability of cyberspace.

The first Cyberstability Paper Series explores these "New Conditions and Constellations in Cyber" by collecting twelve papers from leading experts, each providing a glance into past or future challenges and contributions to cyberstability. The papers are released on a rolling basis from July until December 2021, culminating in an edited volume. All papers will be available for open access, and a limited number of printed hardback copies are available.

Published by

GLOBAL COMMISSION
ON THE STABILITY OF CYBERSPACE

The Hague Centre
for Strategic Studies