Cyberstability Paper Series

New Conditions and Constellations in Cyber

The Evolution of the UN Group of Governmental Experts on Cyber Issues

From a Marginal Group to a Major International Security Norm-Setting Body

Heli Tiirmaa-Klaar
Ambassador for Cyber Diplomacy, Estonian Ministry of Foreign Affairs

December 2021

Cyberstability Paper Series
New Conditions and Constellations in Cyber

The Evolution of the UN Group of Governmental Experts on Cyber Issues from a Marginal Group to a Major International Security Norm-Setting Body

Heli Tiirmaa-Klaar | Ambassador for Cyber Diplomacy,
Estonian Ministry of Foreign Affairs

December 2021

This article offers insights on the major milestones and discussions by the consecutive United Nations Groups of Governmental Experts (GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security. In parallel to addressing the development of cyber norms, the article also analyzes other pertinent regional and global developments during the period 2005–2021, which have formed the geostrategic context for the successive GGEs. It highlights the internal factors and external events that were at play in transforming this relatively marginal UN group in the early 2000s into a central cyber norm-setting body by 2021.

This article offers a depiction of nascent multilateral negotiations on cyber norms by the UN Groups of Governmental Experts to develop the framework for state behavior in cyberspace, which eventually becomes a widely accepted universal rulebook. Against the background of growing concerns stemming from misuse of new technologies to countries' foreign policy and national security, the story of cyber GGEs entails useful lessons for diplomats, decision-makers, and the larger public on how to achieve multilateral agreements on frontier issues of international security.

Heli Tiirmaa-Klaar is Ambassador for Cyber Diplomacy and Director General for the Cyber Diplomacy Department at the Estonian Ministry of Foreign Affairs. She was the expert appointed to the 2019-2021 UNGGE by the Estonian government.

In summary, the GGEs achieved consensus when taking place during a favorable geopolitical context, where tensions between the leading powers were relatively low or there was otherwise a common interest in achieving agreement. The other elements playing a role in the successful outcome of negotiations are comprised of proficiency of the chairs, expectations by the group members, regional dynamics, effective backchanneling efforts, and increasing professionalization of GGE members.

The UN discussions on cyber norms are nearly as old as the World Wide Web itself.[1] The central role of technology in the political-military context became evident in the beginning of the 1990s when the United States gained a dominant position in terms of technological advancement, also manifested in its military supremacy. A short Gulf War in 1991 demonstrated that the use of high-technology conventional weapons has created clear advantages for the U.S. led coalition forces.[2]

Recognizing the U.S. dominance in information and communications technology (ICT), the Russian Federation first proposed to discuss the ICT issues in the context of international security in the UN as early as 1998. After several attempts to use different UN venues to start discussions, it was decided that the best way forward was to create a Group of Governmental Experts (GGE) under the Disarmament Committee. The United Nations General Assembly uses GGEs as a common tool by which to examine emerging security topics relevant to international security, such as transparency and confidence-building measures in outer space activities, or the use of lethal autonomous weapons systems. The Russian Federation proposed a UNGA resolution in 2002 that called for the creation of the GGE to study threats and possible cooperative measures in cyberspace.[3]

It was not until 2007 that the broader public discovered that the cyber domain became a source of strategic risk that could destabilize countries and create large-scale political and economic havoc.

The first GGE on cyber issues gathered under the auspices of the UN Disarmament Committee in 2004–2005. This first attempt did not result in the consensus report for several reasons, among which were the unwillingness of the UN Security Council permanent members to agree on the direction of the report, and the lack of broader international interest toward cyber stability issues at that time.

According to several different accounts on the history of cyber conflict, the period before 2007 featured low levels of cyber threat awareness among top decision-makers, diplomats, and military leaders. Serious cyber intrusions into military systems and cyber intelligence operations rarely made any headlines, but stayed in the confines of national security-related confidential files.[4] During this period, cybersecurity was generally seen as a technical issue, a task for information security management teams and IT departments both in the public and the private sectors.

It was not until 2007 that the broader public discovered that the cyber domain became a source of strategic risk that could destabilize countries and create large-scale political and economic havoc. During the "bronze soldier monument" events in Estonia, the country experienced a Russian hybrid campaign aided by the first publicly known large-scale cyber operation that resulted in many online targets in Estonia being subjected to a state of digital siege. In retrospect, the Estonian events served as a wake-up call that demonstrated how cyberattacks and hybrid operations can be used in a geostrategic context for advancing foreign policy goals.

It should be noted that in 2007 Estonia was already one of Europe's most wired countries, with many private and public sector services available online. It had, for instance, introduced a na-

tion-wide digital authentication system used by the majority of the population. Several waves of cyberattacks, most of them in the form of DDoS (Distributed Denial of Service) attacks, targeted media outlets, online banking, and governmental websites.[5] During the three weeks of cyber siege, the Estonians were forced at some point to limit their connectivity to the World Wide Web in order for the Internet services inside the country to continue, and only locals could still carry out essential transactions online as they were accustomed to doing. Targets of the DDoS attacks were mostly websites, and the cyber operations stayed away from the electricity, transport, industrial control systems, and military networks. Except for online banking services and governmental websites, the botnets that were employed did not target civilian critical infrastructure, i.e., malicious cyber activities clearly stayed below the threshold of an armed attack.

Although this hybrid campaign originating from the relocation of a Soviet WWII monument had many elements, the cyberattacks received much wider international media attention compared to organized riots in the streets and the physical blockading of the Estonian Embassy in Moscow or the closing of the land border to Russia to transit flows. The 2007 Estonian cyber siege is widely known as the first significant cyber event, and has catapulted the formerly technical cyber issues into the limelight. Never before had large-scale cyberattacks been used to "punish" a country for activities that run against the foreign policy interests of another country. This event put cybersecurity onto the map of foreign and security policy senior decision-makers, and marked a starting point for cyber issues becoming increasingly mainstreamed to a more strategic level, both nationally and internationally.

In 2006–2008, several notable cyber incidents took place against the U.S. and European governmental networks, as well as private-sector targets, especially the banking and oil sectors.[6] Reporting on cyber incidents grew, and the policymakers became aware of the need to find commonly accepted rules that would set boundaries of state activities in cyberspace. A new kind of visible cyber operation was conducted by Russia during the short war between Russia and Georgia in 2008. Although technologically not too sophisticated, but nonetheless effective, the DDoS and defacement attacks against Georgian media outlets and governmental websites were taken out of the same playbook as attacks on Estonia a year earlier.[7] The operation against Georgia was in support of the overall objective to cut off strategic communication capabilities during the first days of conflict and discredit the country internationally. Again, these cyberattacks became widely known and published in the world media.

After the events in Georgia in 2008, cyber threats undeniably became security and foreign policy concerns, and policymakers started to look for venues where the question of setting acceptable state behavior in cyberspace could be raised. Interestingly, in 2006 a new UNGA resolution had been proposed by the Russian Federation to create a new GGE in 2009.[8] Ironically, the UN member states' growing support of the Russian annual UNGA resolutions on developments in the field of ICTs in the context of international security was facilitated by the number of significant attacks against their networks.

Following these events, the GGE process started to gain in maturity. The second UN GGE started in 2009 with the mission "...to continue to study existing and potential threats in the sphere of information security and possible cooperative measures to address them."[9] The process of setting boundaries for state behavior in cyberspace now truly began against the background of a growing number of significant cyber incidents.

The 2010 GGE report recognizes that cyber threats "...are among the most serious challenges of the twenty-first century...their effects carry significant risk for public safety, the security of nations, and the stability of the globally linked international community..."[10] The 2009–2010 GGE negotiations led to a recommendation that further dialogue among states is necessary to reduce risk and protect critical infrastructure. The recommendations sections also called for "confidence building, stability, and risk reduction measures to address the implications of state use of ICTs."[11] The 2010 report is a short one, consisting of threats, cooperation measures, and recommendations. Allegedly, there was a longer report prepared but discarded at the last minute. Nevertheless, consensus was found to continue discussions and the report has paved the way to more fruitful GGEs in the future.

Although the process was regarded as very important by a handful of cyber connoisseurs in the foreign ministries and nascent cyber forces, the larger public policy and national security community were still generally unaware of this group gathering "somewhere in the UN basement," as one cyber expert participating in discussions called it. More than the report itself, the 2009–2010 process was an important vehicle for forming a nascent international cyber community coalescing around this issue, and it defined a group of nations that were dedicating time and resources to figuring out international policy for regulating state behavior in cyberspace. It also created a precedent for cyber issues to be discussed in the UN First Committee agenda as part of international security, taking it further from the perception that cybersecurity is limited to a dusty server room. Some participants also characterized these early days as creating "positive tension" between technical cyber geeks and non-technical policy wonks, helping to show that the wonks also had something valuable to offer to this field.

The GGE of 2012–2013 took this one step further and produced a very solid and coherent report. The document references all four major elements that will later be declared as a framework for responsible state behavior in cyberspace.[12] These include the application of existing international law, voluntary non-binding peacetime norms of responsible state behavior, confidence and cooperation measures, and capacity-building measures. The report also introduced a chapter on threats, risks and vulnerabilities, and mentioned the role of regional organizations in advancing cyber cooperation.

The 2013 report is best known for its strong affirmation of the international law obligations to state behavior in cyberspace. It claims that international law, and in particular the UN Charter as well as the Universal Declaration of Human Rights, apply in cyberspace. The report goes further in establishing that "the application of norms derived from existing international law relevant to the use of ICTs by states is an essential measure to reduce risks to international peace, security, and stability."[13] Paragraph 23 of this report captures three key obligations for state behavior that are still very relevant: "States must meet their international obligations regarding internationally wrongful acts attributable to them. States must not use proxies to commit internationally wrongful acts. States should seek to ensure that their territories are not used by non-state actors for unlawful use of ICTs."[14]

The question of the applicability of international law has been an especially controversial one since the start of the GGE discussions. The Western likeminded governments have always stressed the applicability of the existing international law, which needs to be applied in the cyber context. The key obligations for state behavior in peacetime, mentioned in the previous paragraph, are derived from the existing international law. The UN Charter and International Humanitarian Law provide sufficient guidance for state behavior in times of conflict, both in jus ad bello and jus in bellum. It was

expected that states develop legal norms codified by these existing bodies of law, and that this would have a tremendous stabilizing effect on cyberspace.

However, the Russian Federation proposed a Code of Conduct on Information Security as early as 1998 that calls for a special UN instrument to include different measures that would bolster information security.[15] The same proposal with some updates was repeated by China and Russia in 2011, and again by the members of the Shanghai Cooperation Organisation in 2015, this time also including a recommendation to change the current Internet model that would give governments an upper hand on Internet governance instead of the multistakeholder community.[16] As the Western governments feared the Code would facilitate further content control, changes in Internet governance, and would mostly be used for legitimizing censorship by authoritarian regimes,[17] they have strongly opposed an emergence of a legally binding instrument during the UN First Committee discussions. The conversation around international law has been a central preoccupation of all GGEs after 2013, and was one of the root causes for the failure to find consensus in 2017.

In retrospect, the 2013 GGE report paved the way for a more advanced 2015 report that still remains a gold standard for setting boundaries of state behavior in cyberspace through its eleven non-binding voluntary peacetime norms for responsible state behavior. When these norms were negotiated in 2015, the participants in the room could not have known that their work would establish a central framework by which to regulate state cyber behavior for the next decade. These norms include additional commitments by states to cooperate, assist, and consult in cases of cyber incidents, to refrain from activities that can affect critical infrastructure, and to abide by a specific norm to protect computer incident response teams, which should not be attacked and should themselves not engage in malicious cyber activities. It also mentions attribution, supply chain and vulnerability disclosure as new elements compared to the 2013 report. In addition, the report makes substantial recommendations on confidence and capacity-building measures.

Among other areas of professionalization of the GGE discussions, a more nuanced separate section on applying international law was added to the 2015 report. It repeats some of the obligations mentioned in 2013, but also mentions new elements, such as the principles of humanity, necessity, proportionality, and distinction from the International Humanitarian Law (IHL). The IHL itself is not mentioned due to an argument by one GGE expert that if the jus in bello body of law will be cited it legitimizes the use of cyberspace for military purposes. A majority of the observers does not see a direct link in how recognizing the IHL applicability can militarize cyberspace, but this has been a long-standing argument by experts from China and has complicated international law discussions in many GGEs.

After the 2015 consensus was achieved, it left everyone a little disappointed, but was still (or because of that) praised as a major step forward in retrospect. Negotiations in 2016 started with an understanding that the new report should add recommendations on how to implement norms of responsible state behavior. However, the 2016–2017 GGE process did not bring consensus for several reasons, among which was disagreement on international law. One of the central elements for the failure was a worsening geostrategic relationship between major powers due to the Russian interference in the U.S. presidential elections in 2016.

The collapse of the 2016–2017 GGE created a collective wound, especially since the number and sophistication of cyber operations had grown exponentially, leaving states to wonder how they can use international mechanisms to better protect themselves and to respond more effectively to

malicious cyber activities. Although the regional organizations (OSCE, ARF, OAS, etc.), the Global Commission on the Stability of Cyberspace (GCSC), and other multistakeholder fora were attempted to fill the cyber norm-creation vacuum, without the formal UN umbrella it did not have the same diplomatic weight, albeit they all provided a very valuable addition to the global cyber debate.

In the Fall of 2018, the international cyber community confronted the UNGA73 season with new enthusiasm to re-establish the cyber norms debate in the First Committee. Despite the newly found optimism, it was quite clear that the drama that led to the failure in 2017 was still casting its shadows on UN cyber negotiations. There were two cyber resolutions on the table in 2018, one by the U.S. and one by Russia. The U.S. resolution was calling for the creation of the new GGE to provide an additional understanding of how the agreed norms could be implemented, and called for issuing a separate annex with national contributions on how the international law applies in cyberspace.[18]

In this resolution, the controversial issue of international law was parked outside the report with the hope that it would make consensus-building easier later. As a post-factum note, the annex on international law was still one of the last critical open questions until the very end of negotiations, before reaching consensus during the most recent GGE in 2021.

While the U.S.put forward a resolution for a new GGE, Russia had a new initiative in mind. The Russian resolution contained a mix of different old and new paragraphs, some not too much related to the cyber context. But the text called for the creation of the inclusive Open Ended Working Group (OEWG) that created a possibility to have a seat at the cyber table for all UN states—a prospect that many found attractive.[19] Further, unlike the GGE, the OEWG promised to at least "consult" non-state experts—although this factor was heavily diluted during implementation.

The idea of the new OEWG was not overly popular among the liberal democratic like-minded nations in the beginning, as it raised again the questions of the actual motives for the creation of the new group, and whether the OEWG would become a battlefield between two different visions of the future of cyberspace, democratic and autocratic. The fears of introduction of a new legal instrument re-emerged as did memories of other difficult discussions from previous GGEs. The tension was somewhat eased after careful selection of chairs to both processes, who were experienced Brazilian and Swiss diplomats. With the choice of neutral chairs, hope was restored that objectivity would prevail in the First Committee cyber discussions. To manage the two parallel groups, UNODA was in a difficult position to come up with a schedule of OEWG and GGE sessions that would facilitate a coordinated approach. An overall concern was how to create complementarity between the two groups, instead of competing processes.

In September 2019, all nations participating in GGE 2019–2021 entered the first substantive OEWG discussion in New York with well-prepared dossiers, ready to stand up for the achievements of previous GGEs and, if needed, eager to defend the added value of the current GGE. In fact, already during the first days of the OEWG session, most of the newcomers at the table from the wider UN membership repeated the mantra: "We are not starting here from scratch, but will build this OEWG process on already achieved consensus by previous GGEs." It became evident that the important four tenets cemented by previous GGEs had become a clear guiding framework for all nations, who were just happy to have a seat at the UN cyber table finally, and were not particularly keen to be regarded as puppets of the OEWG originator. The European Union member states also brought the EU jargon of commonly agreed legal basis, "acquis," to the UN context to signify the consensus by previous GGEs.

After the first meeting in September 2019, the initial weariness about the formation of the OEWG gave way to cautious hope on the possibility to have two complementary processes that serve slightly different objectives. The GGE was expected to create an additional layer of understanding of norms of responsible state behavior and would be driven by a relatively small group, whereas the OEWG would become an inclusive awareness-raising and socializing body on the existing consensus on international law, norms of responsible state behavior, confidence-building measures, and capacity building.

It became evident that the important four tenets cemented by previous GGEs had become a clear guiding framework for all nations, who were just happy to have a seat at the UN cyber table finally.

The first GGE session in New York in December 2019 was a friendly gathering of experts, old and new, who were almost exclusively senior-level diplomats or civil servants with important cyber policy roles. When choosing GGE members, the UN Secretary General had tasked UNODA to seek, in addition to regional balance, also a gender balance. The gender balance was certainly more equal in this GGE round, and served as an important element that contributed to the success of the group as observed by one GGE expert.

The first two GGE meetings were running relatively smoothly until the second session in Geneva in 2020, after which the pandemic struck and changed everything. Both the GGE and OEWG moved to virtual meeting rooms with an uncertain prospective of their outcomes.

Due to difficulty in managing meetings in a way that experts from all time zones could attend during business hours, the meetings took place during European, African, Middle Eastern, and American working hours. Many of the Asia-Pacific GGE experts had to work in the middle of night, and endure the whole week with little sleep as they also had to fulfil their responsibilities during the working day. Despite all these complexities, the sessions were very professional and substantive, allowing enough face time for the experts to react to other experts, and room for the chair to maneuver through the difficult questions. Participants applauded the always calm and diplomatic Brazilian chair, Ambassador Guilherme Patriota, who was stuck in Mumbay as the Brazilian Consul General during the whole pandemic and managed to keep the online sessions of GGEs running.

Although the pandemic brought major disruptions to GGE experts' routine lives and strained the work schedules with too many online events, it also allowed for more sessions than usual. The resulting report of the 2019–2021 GGE could be characterized as a rare victory of multilateral diplomacy where all parties to negotiations felt that they had won something. For the Western nations, important mentions of international law were included in the report as well as substantial paragraphs on attribution and explanations on critical infrastructure protection norms. The attached compendium on international law has created a solid collection of national views on this central issue. China walked away with the desired text on supply chain, and Russia was able to get in the sentence on new OEWG. Developing nations were also satisfied with the report on further cooperation, consultations, and capacity-building points.

In order to analyze what factors aided the process of building consensus in 2019–2021, the leading drafter in the GGE secretariat, Camino Kavanagh from the UNIDIR support team, has attributed the success to many favorable factors that were mutually reinforcing, especially the work done by the chairs and the secretariat that allowed for coordination of the draft reports, as well as timing of the events.[20]

It should be noted that many saw the parallel processes as two sides of the same coin. This "hostage situation" was nerve-racking for all states who were looking forward to having clear guidance by the United Nations and who wanted to see results in both processes.

The Australian GGE expert, Johanna Weaver, praised the high quality of work by the secretariat and chairs, and observed the overall desire by nations to achieve consensus recommendations as a result of the first inclusive UN cyber format, which could then be replicated in a smaller GGE group in a more detailed manner: "The OEWG was a success because at the last meeting we had an excellent draft on the table and 'middle-ground' countries had repeatedly and publicly underscored that no-outcome was not an option. This helped apply pressure to bring the 'great powers' to the table; no great (or less great) power wanted to be the one to cop the blame for getting in the way of a defensibly good report that everyone wanted."[21]

On reaching the consensus in the 2021 GGE, she observed: "The final GGE meeting occurred after the inaugural OEWG concluded, but just days before the organizational session of the new OEWG. This, combined with dynamics that flowed from other unrelated but concurrent UN fora, as well as geopolitical goings-on external to the UN, all aligned to create a climate where consensus was within reach. We had another excellent draft on the table. In the final hours, it would be wrong to say that all interests aligned, but everyone needed something, and we were able to find a way to give each what they needed without impinging on others redlines."[22]

In successful international negotiations, there are usually many coinciding elements that have come together in certain points of time and produced a desired outcome. This was also the case with all successful GGE outcomes, where internal GGE group dynamics and other factors coincided with a broader enabling strategic environment.

The 2009–2010 process was regarded as the first successful GGE that allowed the work to continue on shaping international cyber norms and created the community of nations interested in the topic. However, it is also very important to note that the new U.S. administration had been inaugurated in 2009, which changed the direction of the U.S. cyber policy that facilitated reaching the GGE goals. President Obama had issued its Cyberspace Policy Review in May 2009 with recommendations on both national and international activities.[23] This gave the U.S. diplomats a green light with which to engage in the UN discussions.

During the 2012–2013 GGE negotiations, President Obama and President Putin agreed to establish a new working group within the U.S.–Russia Bilateral Presidential Commission as a part of the cybersecurity confidence-building measures between the U.S. and Russia. Already in early 2011, the U.S. and Russia had started regular discussions on cyber confidence-building measures to avoid accidential escalation, and agreed to establish a U.S.–Russia cyber hotline similar to the nuclear hotline from the Cold War days.[24] This has also faciliated the adoption of the first set of cybersecurity confidence-building measures in the OSCE in 2013.

As a broader enabling factor in 2015, the final GGE session in July preceded the President Obama meeting with Xi Jinping in September 2015, where the bilateral agreement was reached, to not "... knowingly support the cyber-enabled theft of intellectual property, including trade secrets or other confidential business information for commercial advantage."[25]

In 2021, several elements in the ongoing UN First Committee cyber debates could be attributed to positive GGE outcomes, but there was also an overarching political motive for working toward

consensus before the U.S.–Russia Summit that was announced to be taking place in June in Geneva. The announcement on the Summit date came out two days before the GGE final report was concluded on the 28th of May. In a way, the ongoing cyber GGE negotiations became but one piece in a larger geopolitical puzzle that was put together before the summit.

The first U.S. cyber envoy, Christopher Painter, assessed that a wider geopolitical context always played an important role in contributing success to different GGEs:

> "The GGE, like any other development in cyberspace, is tied to the larger geopolitical environment and political will. When geopolitical tensions between Russia and the United States are relatively low and stable, as was the case in 2013, agreement and consensus in the GGE is more likely. When they are very high , as in 2017 because of Russian election interference and other malicious activity, consensus and agreement are unlikely. Yet, this doesn't tell the whole story. Even when larger geopolitical tensions are high between the two countries, they can and have still reached agreement if it is in both of their strategic interests and there is political will. A significant consensus was reached in 2015 despite Russia's invasion of the Ukraine and the consequent suspension of the high-level US–Russia cyber dialogue because both countries saw value in the articulation of a normative framework for cyberspace and the continuation of the GGE. Agreement was reached again in 2021 despite continued poor relations between the US and Russia on both cyber and non-cyber issues. However, as cyber issues continue to be elevated as a national security issue and integrated into broader national security and diplomatic priorities, it is likely that the success or failure of cyber negotiations, like any other negotiations, will increasingly be dependent on the overall relationship between the countries who are major players."[26]

It is essential to note that, in parallel to GGEs taking place in the UN, a number of regional organizations started discussions on cyber confidence-building measures, norms, international law, and capacity building, further mainstreaming the four elements in the GGE reports as a normative basis for state behavior. The OSCE adopted two sets of cyber security confidence-building measures in 2013 and 2016, and continues to implement these measures through its cybersecurity working group.[27] The ASEAN Regional Forum has discussed cyber confidence-building questions since 2012,[28] and the ASEAN ministerial conference on cybersecurity has endorsed the eleven norms of responsible state behavior from the 2015 GGE report.[29] The Organisation of American States has an active Cyber Security Programme facilitating the exchange of best practices, training, and education among all its members, as well as implementation of capacity-building projects.[30] The European Union has mainstreamed the issue of cyber diplomacy into its policy proceedings since the 2013 EU first Cyber Security Strategy.[31] All these regional initiatives have further raised awareness of GGE agreements on cyber norms, confidence-building measures, and international law applicable in the cyber domain. They have also helped to increase global interest toward ongoing UN cyber negotiations, and have created additional expectations for each GGE to progress with discussions in order to provide better guidance for state behavior.

In parallel to GGEs taking place in the UN, a number of regional organizations started discussions on cyber confidence-building measures, norms, international law, and capacity building, further mainstreaming the four elements in the GGE reports as a normative basis for state behavior.

One of the central elements contributing to the success of different GGEs was also the composition of the group, which has determined the discussion dynamics. In earlier years, the composition of the GGEs was a mix of technical cyber experts, military officers, academics, and diplomats. The first GGEs also included a few academics and technical experts, but each successive GGE had more diplomats with international security and arms control backgrounds involved. The gradual professionalization of the "cyber diplomat tradecraft" was noticeable also in the quality and substance of the negotiations. By the 2019–2021 GGE, there were already diplomats with specific cyber expertise who emerged in many MFAs, which made the difference in the quality of discussions. As one of the experts recalls: "It is not so much that there were increasing numbers of diplomats in the room; rather, it was that there were increasing number of diplomats that specialized in cyber policy in the room. There are nuanced differences in cyber policy and arms control. Some skills are transferable, but subject matter expertise—of cyber as a strategic foreign policy issue—is what brought depth to the discussions."[32]

Naturally, there were also principals among the experts who provided steadiness and historical memory for the group. For the cyber diplomats' community, it is quite well known that the continuity of discussions for rules of the road in cyberspace was essentially up to two skillful diplomats, Michele Markoff from the United States and Andrey Krutskyh from Russia. They had been working together already during the Cold War on several disarmament issues, and were founding members of cyber GGEs. The dynamic between the two senior and experienced cyber experts from two superpowers in the room often defined the atmosphere of negotiations. Without the long-standing relationship between them, it would be hard to imagine the GGEs as we know them.

The chairs of each GGE reiteration also played a major role in setting the tone for each group. The 2009–2010 GGE was chaired by Andrey Krutskyh from the Russian Federation, who was the initiator of the whole UN First Committee cyber discussion. In 2012–2013, the chair was a senior Australian diplomat, Deborah Stokes, who was praised for her ability and skills to build consensus. In 2014–2015, the Brazilian chair, Carlos Perez, was known for effective backchanneling between the experts and for solving complex negotiations with personal diplomacy efforts. In 2016–2017, the chair was one of the first European cyber diplomats, Karsten Geier from Germany, who had a high degree of subject matter expertise and tried everything in his power to reach consensus despite the political climate. In 2019, expectations were very high when Ambassador Guilherme de Aguiar Patriota took over the GGE chairmanship. He had outstanding experience in chairing a number of GGEs before, and this was visible in the room where he could skillfully steer discussions, and also virtually, even when some delegates proved to be difficult from time to time.

In addition, there were also UNODA and UNIDIR team members who provided the secretariat for each GGE as well as OEWG, and created consistency between different reiterations of groups. Kerstin Vignard, James Lewis, Camino Kavanagh, and Gillian Goh were key players behind the scenes who brought difficult drafting processes to a victorious end.

It would be unfair not to mention a significant negotiator who was instrumental in bridging the OEWG and GGE discussions to achieve consensus in the final rounds of March to May of 2021. The Australian GGE expert, Johanna Weaver, worked magic in New York in the spring of 2021 and facilitated sometimes tough negotiations between UN member states in the final stages of the two working groups. During the ongoing pandemic, with limited international travel, she was volunteering to establish a presence in New York for three months and proved especially efficient in arbitraging final GGE disputes between key players.

Looking at the composition of the each GGE, there were many other outstanding cyber experts and diplomats, all of whom played key roles in the process and provided valuable contributions to each GGE.[33] As the cyber issues gained more relevance to foreign and security policy, the group grew from the initial fifteen members to twenty-five by 2021. The UN Security Council's permanent five members were always present in the group, leaving few seats left over, for which countries were competing intensely each time a new GGE emerged. Picking the members of the group was always a complex process, where, in addition to regional balance, the cyber expertise and negotiating experience of each expert was evaluated by UNODA.

As the analysis above demonstrates, each different GGE took place in a specific geostrategic context and was influenced by many simultaneous dynamics. It requires further in-depth analysis to determine what exactly brought success or failure to each GGE process, due to the complexity of international multilateral negotiations as there were many influential factors behind the scenes that are rarely known to the wider public. The history of cyber GGEs certainly deserves a longer account that would also include the memoirs of key players, and more substantive analysis than the short format of this article allows. Michele Markoff suggests that successful outcomes were brought by "common interest in preventing conflict and an atmosphere conducive to political will and collaboration."[34]

The conclusion can be made that the GGEs achieved consensus when taking place during a favorable geopolitical context, where tensions between the leading powers were relatively low or there was otherwise a common interest in achieving agreement.

In very general terms, the conclusion can be made that the GGEs achieved consensus when taking place during a favorable geopolitical context, where tensions between the leading powers were relatively low or there was otherwise a common interest in achieving agreement. Other elements playing a role in the successful outcome of negotiations are comprised of proficiency of the chairs, expectations by the group members, regional dynamics, effective backchanneling efforts, and increasing professionalization of GGE members.

Conclusion

With six GGEs from 2004 to 2021, a solid foundation is built for more predictable state behavior. Four elements discussed above, including the application of existing international law, voluntary non-binding peacetime norms, confidence building, and capacity-building measures form a normative framework for responsible state behavior. Different iterations of GGEs that have developed norms and guidance on norm implementation as well as the OEWG recommendations have brought the international cyber community to a good place by the end of 2021. Now the challenge of implementation of these recommendations lies ahead. The next milestone for the First Committee cyber discussions will be a first substantive session of the new Russian-proposed OEWG in December 2021. There is also a proposal for the Programme of Action presented by France and Egypt and co-sponsored by more than fifty countries with the ambition to steer the operationalization of the recommendations. It is hard to predict which process will be more efficient in the long run, but it is quite clear that there are many UN member states that still need to build expertise on how to implement cyber norms and apply international law.

Endnotes

1 This is using the definition of the World Wide Web that has arisen with the widespread introduction of websites and web browsers after 1994/1995.

2 Gene Rochlin and Chris Demchak, "The Gulf war: technological and organizational implications," Survival 33, no. 3 (May/June 1991): pp 260–273, https://www.tandfonline.com/doi/abs/10.1080/00396339108442594.

3 United Nations General Assembly, "Resolution adopted by the General Assembly on Developments in the Field of Information and Telecommunications in the Context of International Security" A/RES/56/19, United Nations, January 7, 2002. https://digitallibrary.un.org/record/453522?ln=en#record-files-collapse-header

4 Jason Healey, "A Brief History of US Cyber Conflict" in Healey ed. A Fierce Domain: Conflict in Cyberspace, 1986 to 2012 (Cyber Conflict Studies Associated Publication, in Partnership with the Atlantic Council, 2013): pp. 15–40.

5 Andreas Schmidt "The Estonian Cyberattacks," in Healey ed. A Fierce Domain: Conflict in Cyberspace, 1986 to 2012 (Cyber Conflict Studies Associated Publication, in Partnership with the Atlantic Council, 2013).

6 "Significant cyber incidents since 2006," Center for Strategic and International Studies, accessed 24.10.2021, https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents

7 "Georgia-Russia Conflict 2008," CCDCOE, accessed 24.10.2021, https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents

8 United Nations General Assembly, "Resolution adopted by the General Assembly on 6 December 2006 on Developments in the Field of Information and Telecommunications in the Context of International Security," A/RES/61/54, United Nations, December 19, 2006. https://undocs.org/A/RES/61/54

9 Ibid.

10 United Nations General Assembly, "Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security," A/68/98, United Nation, June 24, 2013. https://undocs.org/A/68/98

11 Ibid.

12 Ibid.

13 Ibid.

14 Ibid.

15 For further analysis on how the Russian and Western approaches differ on cybersecurity, see Alexander Klimburg, The Darkening Web: the War for Cyberspace, (New York: Penguin Books: NY, 2017): pp.117–129.

16 United Nations General Assembly, "Letter dated 9 January 2015 from the Permanent Representatives of China, Kazakhstan, Kyrgystan, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General", A/69/723, United Nations, January 13, 2015. https://undocs.org/A/69/723

17 John Markoff and Andrew Kramer, "U.S. and Russia Differ on a Treaty for Cyberspace", New York Times, June 27, 2009, https://www.nytimes.com/2009/06/28/world/28cyber.html

18 United Nations General Assembly, "Resolution adopted by the General Assembly on 22 December 2018 on Advancing responsible State behaviour in cyberspace in the context of international security," A/RES/73/266, United Nations, January 2, 2019. https://undocs.org/A/RES/73/266

19 United Nations General Assembly, "Resolution adopted by the General Assembly on 5 December 2018 on Developments in the field of information and telecommunications in the con-

text of international security", A/RES/73/27, United Nations, December 11, 2018. https://undocs.org/en/A/RES/73/27

20 "The positive outcome of the OEWG and GGE was due to a combination of factors. These include the commitment of UN member states and experts; the continuity provided by the common secretariat which supported both chairs and processes; diplomatic skills and coordinated approach to both processes by two chairs; the engagement of multiple actors in the processes enabled by both resolutions and their provisions for consultations; and broader diplomatic developments which contributed to making the environment more conducive to positive outcomes." Interview with Camino Kavanagh, a member of UN GGE and OEWG secretariat on 21 September 2021.

21 Interview with Johanna Weaver, former Head of Australian Delegation to the UN OEWG and GGE on 21 October 2021.

22 Ibid.

23 "The Comprehensive National Cybersecurity Initiative," White House President Barack Obama, accessed on October 24, 2021, https://obamawhitehouse.archives.gov/issues/foreign-policy/cybersecurity/national-initiative

24 Timothy Farnsworth, "US, Russia to Discuss Cyber Hotline," Arms Control Association, accessed on October 24, 2021, https://www.armscontrol.org/act/2012-05/us-russia-discuss-cyber-hotline

25 "Remarks by President Obama and President Xi of the People's Republic of China in Joint Press Conference", White House President Barack Obama, September 25, 2015. https://obamawhitehouse.archives.gov/the-press-office/2015/09/25/remarks-president-obama-and-president-xi-peoples-republic-china-joint

26 Online linterview with Christopher Painter, the former U.S. State Department Cyber Coordinator on 26 October 2021.

27 See more detailed information on the OSCE cyber activities at "Cyber/ICT Security", OSCE, https://www.osce.org/secretariat/cyber-ict-security

28 "Annex 11. ASEAN Regional Forum Experts and Eminent Persons (ARF/EEP) Recommendations for ARF Initiatives on Promoting Cyber Security," ASEAN Regional Forum, March 6, 2018, at https://aseanregionalforum.asean.org/wp-content/uploads/2019/01/ANNEX-11-ARF-EEP-FINAL-REPORT.pdf

29 Elina Noor, "ASEAN Takes a Bold Cybersecurity Step," The Diplomat, October 4, 2018, https://thediplomat.com/2018/10/asean-takes-a-bold-cybersecurity-step/ .

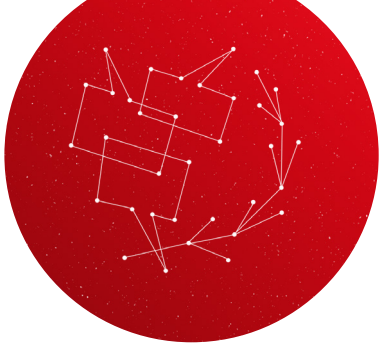
30 "Cybersecurity program", OAS, https://www.oas.org/en/sms/cicte/prog-cybersecurity.asp

31 European Commission, "JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS. Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace", European Union, February 7, 2013. https://op.europa.eu/en/publication-detail/-/publication/e8ab3970-f86e-41a6-8666-33e94614dcf2/language-en

32 Interview with Johanna Weaver, former Head of Australian Delegation to the UN OEWG and GGE on 21 October 2021.

33 The composition of each GGE is described in reports and can be accessed at "Group of Governmental Experts," United Nations, https://www.un.org/disarmament/group-of-governmental-experts/

34 Online linterview with Michele Markoff, the U.S. State Department Acting Coordinator for Cyber Affairs on 18 November 2021.



About the Author

Heli Tiirmaa-Klaar is Ambassador for Cyber Diplomacy and Director General for the Cyber Diplomacy Department at the Estonian Ministry of Foreign Affairs. Up to Fall 2018, she was working as a Head of Cyber Policy Coordination at the European External Action Service where she steered and coordinated EU external relations on cyber issues since 2012. She set up EU strategic cyber dialogues with the US, India, Brazil, Japan, South Korea as well as other international organisations. She also kicked off EU global cyber capacity building programs and steered the development of the EU Cyber Diplomacy Toolbox to bolster EU response to malicious cyber activities. In 2011, she was assigned to the NATO International Staff to prepare the NATO Cyber Defence Policy.

She has been working on cyber security since 2007 when she led the development of the Estonian Cyber Security Strategy. In 2008-2010 she coordinated the implementation of the Estonian strategy, managed the National Cyber Security Council and led the establishment of Estonia's national cyber resilience structures as well as public-private partnerships for cyber security. In her earlier career, she held various managerial positions at the Estonian Ministry of Defence and the Tallinn University. She was a Fulbright Scholar at the George Washington University and has published in several academic journals throughout her career.

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