9

Building Cyber Peace While Preparing for Cyber War

Frédérick Douzet, Aude Géry, and François Delerue

Since President Macron's launch of the Paris Call for Trust and Security in Cyberspace in the fall of 2018,[1] amidst the collapse of international cyber norm discussions in June 2017, the international community has contemplated and launched multiple initiatives to restore a multilateral dialogue on the regulation of cyberspace in the context of international security. In December 2018, two resolutions were adopted by the United Nations General Assembly to set up two processes on progress in information and telecommunications in the context of international security: The sixth Group of Governmental Experts (GGE)[2] on the subject and a new Open-Ended Working Group (OEWG).[3] Then in October 2020, a few months before the end of these two processes, France and Egypt, together with thirty-eight countries and the European Union, proposed the launch of a program of action for advancing responsible state behavior in cyberspace,[4] while two new resolutions were once again adopted by the UN General Assembly.[5]

At first sight, this profusion of initiatives looks like a renewed and strong interest among states in advancing cyber peace and stability. But the details reveal a more complex – and confusing – picture. Competing processes with overlapping mandates and agendas reflect the heightened strategic competition that prevails between great powers that pursue somewhat conflicting goals: Minimizing the risks to international peace, security, and cyber stability while maximizing their own cyber power, security, and normative influence. In other words, the cyber arms race is on and even though states aim at preserving collective security they are not ready

[1] *Paris Call for Trust and Security in Cyberspace*. (2018, November 12). Paris Call. https://pariscall.international/en/.

[2] UNGA Res. 73/266 (Dec. 5, 2018).

[3] UNGA Res. 73/27 (Dec. 22, 2018).

[4] *The Future of Discussions on ICTs and Cyberspace at the UN*. (2020, October 30). UNARM. https://front.un-arm.org/wp-content/uploads/2020/10/joint-contribution-poa-the-future-of-cyber-discussions-at-the-un-10302020.pdf.

[5] UNGA Res. 75/240 (Dec. 31, 2020).

https://doi.org/10.1017/9781108954341.009 Published online by Cambridge University Press

to give up any of their ability to conduct offensive operations in cyberspace.[6] The road to cyber peace is paved with malicious intentions.

This chapter offers an analysis of the multilateral efforts conducted over the past decade to build cyber peace in a context of proliferation of cyber conflicts and exacerbated geopolitical tensions, not to mention the global COVID-19 pandemic that has largely disrupted international meetings. It studies more specifically how international law has been leveraged in UN negotiations to serve strategic objectives. International law plays a central role in state-level discussions on peace and stability in cyberspace, but it has been a source of tension since the very first resolution of the UNGA on the regulation of cyberspace in 1998. Although considerable progress has been made by previous GGEs – notably in 2013 and 2015 – in achieving consensus over the applicability of international law to cyberspace, fundamental disagreements persist that are grounded in conflicting geopolitical representations and interests.

States not only have opposing views on the necessary means to ensure security and stability in cyberspace, but also on the content of the negotiations themselves. This reflects their diverging perceptions of the risks associated with the militarization of cyberspace and with the possible forms of responses authorized by international law in reaction to internationally wrongful acts. It also reflects the entanglement of the issues at stake: Negotiating on protective principles, such as the principle of sovereignty, for example, which may limit states' actions on the territory of other states, bears potential consequences that could extend to the lawfulness of the collection of transborder evidence.[7]

The first part of the chapter explains the context in which the two competing 2018 UN processes were created and, second, examines the challenging – and largely overlapping – mandates they were given. It then analyzes the October 2020 state initiatives as a window into the geopolitical underpinnings of cyber peace building going forward.

1 THE SHORT HISTORY OF CYBER PEACE BUILDING

The OEWG and the sixth GGE were created by resolutions 73/27 and 73/266, adopted within a few days, on December 5 and 22, 2018, respectively, in a context of heightened tensions between states. For the first time since the discussion started in 1998, two resolutions on ICTs in the context of international security – instead of one – were adopted by the General Assembly. While their composition and calendar differ, their mandates are largely similar, making them competing processes in essence. This situation testified to an apparent division between two blocks of member states opposing each other on this topic.

[6] Douzet, F. (2020), *Cyberspace: the New Frontier of State Power.* In Moisio S. et al. (Eds.), *Handbook on the Changing Geographies of the State: New spaces of geopolitics* (pp. 325–338), Cheltenham, UK: Edward Elgar.

[7] Delerue, F., Douzet, F. & Géry A. (2020), *The Geopolitical Representations of International Law in the International Negotiations on the Security and Stability of Cyberspac*e, IRSEM/EU Cyber Direct, pp. 50–55.

https://doi.org/10.1017/9781108954341.009 Published online by Cambridge University Press

Their creation followed a series of preceding GGEs and of UN-level discussions on progress in information and telecommunication in the context of international security that reached a dead-end in June 2017 with the failure of the fifth GGE, triggering a series of private sector and multistakeholder initiatives to maintain international discussions on the security and stability of cyberspace.

The history of cyber peace building is still young but its analysis helps to measure the progress that has been made so far, and the scope of what remains to be done.

1.1 *How Cyberspace Became an International Security Issue in Multilateral Negotiations*

In 1998, the Russian Federation introduced the theme of "Progress in information and telecommunication in the context of international security" at the United Nations General Assembly, initiating a multilateral discussion on the consequences of the development of state and nonstate actors' cyber capacities on international security and stability (UNGA, Report of the First Committee, A/53/576 (1998)). This initiative led to the adoption of resolution 53/70 on December 4, 1998, by the General Assembly, which has since passed a resolution on the matter every year.

These resolutions created five successive GGEs up to 2016 (2004, 2009, 2012, 2014, and 2016). But the participants in the first GGE in 2004 proved unable to reach a consensus on a final report. As one of the experts in the Russian delegation later testified: "whether humanitarian international law and international law provided a sufficient regulation of security in international relations in case of a 'hostile' use of information and communication technologies for politico-military reasons was the main stumbling block."[8] Hence, international law was, from the start, at the heart of the disagreements among governmental experts.

The following three GGEs, however, were successful and led to the adoption of consensual reports in 2010,[9] 2013[10] and 2015[11]. These reports were submitted to the General Assembly by the Secretary General. The UNGA took note of the reports and suggested that member states draw from them.[12] The GGE reports contain recommendations on confidence building measures prone to preserve the security

[8] Streltsov, A. A. (2007), *International information security: description and legal aspects. ICTs and International Security*. Disarmament Forum, p. 8.

[9] UNGA, *Report of the Group of Governmental Experts on developments in the field of information and telecommunications in the context of international security*, A/65/201 (2010).

[10] UNGA, *Report of the Group of Governmental Experts on developments in the field of information and telecommunications in the context of international security*, A/68/98 (2013).

[11] UNGA, *Report of the Group of Governmental Experts on developments in the field of information and telecommunications in the context of international security*, A/70/174 (2015).

[12] UNGA Res. 65/41 (Dec. 8, 2010); UNGA Res. 68/243 (Dec. 27, 2013); UNGA Res. 70/237 (Dec. 23, 2015).

https://doi.org/10.1017/9781108954341.009 Published online by Cambridge University Press

and stability of cyberspace, along with measures of international cooperation and assistance that could be implemented by the states and, most importantly, norms of responsible state behavior in cyberspace.

The first major breakthrough was the recognition of the applicability of international law to cyberspace in the 2013 final report:

> International law, and in particular the Charter of the United Nations, is applicable and is essential to maintaining peace and stability and promoting an open, secure, peaceful, and accessible ICT environment.[13]

As a result, the following GGE was, for the first time, instructed to deal with international law.[14] Its final report in 2015 dedicated a full section (part 6) to international law, listing several rules. Since then, numerous states have endorsed this approach in their voluntary contributions to the Secretary General of the United Nations.[15]

The fifth GGE, however, ended in failure in June 2017, amid a dispute over the interpretation of international law. The governmental experts were indeed not able to reach an agreement for the adoption of a consensual final report. Three states – China, Cuba, and Russia – refused the explicit mention in the final report of the applicability of certain branches of international law, namely, the right of self-defense, the law of countermeasures, and the law of armed conflict. Cuban and Russian governmental experts explained that the endorsement of the applicability of these branches of international law in cyberspace could serve to justify the militarization of cyberspace,[16] and they pointed at profound divergences in interpreting the law. This mention was regarded as crucial by other states, particularly the United States, which released an unusually bitter communiqué blaming "some

[13] UNGA, *Report of the Group of Governmental Experts on developments in the field of information and telecommunications in the context of international security*, A/68/98, at ¶ 19 (2013).

[14] UNGA Res. 68/243 (Dec. 27, 2018).

[15] UNGA, *Developments in the field of information and telecommunications in the context of international security. Report of the Secretary General*, A/68/156/Add.1 (2013); UNGA, *Developments in the field of information and telecommunications in the context of international security: Report of the Secretary General*, A/69/112 (2014); UNGA, *Developments in the field of information and telecommunications in the context of international security: Report of the Secretary General*, A/69/112/Add.1 (2014).

[16] Representaciones Diplomáticas de Cuba en El Exterior (2017, June 23), 71 UNGA: *Cuba at the final session of Group of Governmental Experts on developments in the field of information and telecommunications in the context of international security*. http://misiones.minrex.gob.cu/en/un/statements/71-unga-cuba-final-session-group-governmental-experts-developments-field-information; Ministry of Foreign Affairs of the Russian Federation. (2017, June 29). *Response of the Special Representative of the President of the Russian Federation for International Cooperation on Information Security Andrey Krutskikh to TASS' Question Concerning the State of International Dialogue in this Sphere, Ministry of Foreign Affairs of the Russian Federation*. www.mid.ru/en/main_en/-/asset_publisher/G51iJnfMMNKX/content/id/2804288.

https://doi.org/10.1017/9781108954341.009 Published online by Cambridge University Press

participants" for the failure of the negotiations.[17] The representative of the United States was adamant:

> I am coming to the unfortunate conclusion that those who are unwilling to affirm the applicability of these international legal rules and principles believe their States are free to act in or through cyberspace to achieve their political ends with no limits or constraints on their actions. That is a dangerous and unsupportable view, and it is one that I unequivocally reject.[18]

The deadlock led a number of diplomats to claim that China and Russia were back tracking on the applicability of international law to cyberspace – which both countries denied – and that the discussion should continue among like-minded countries. The dreary perspectives over international discussions encouraged non-state actors to jump in, given the explosion of confrontation in cyberspace and its increasingly damaging consequences.

1.2 *A Multistakeholder Push to Reign in State Behavior*

The Snowden revelations in 2013 uncovered the extent of state offensive activities in cyberspace and made the security and stability of cyberspace a widely public and highly political issue, provoking the first summit bringing together the Internet governance community with the international security community: The so-called Net Mundial conference in 2014. The conference produced a statement with recommendations on Internet governance principles and a roadmap for the future evolution of the Internet governance ecosystem. This non-binding document was "the outcome of a bottom-up, open, and participatory process involving thousands of people from governments, the private sector, civil society, the technical community, and academia from around the world."[19] Since then, the proliferation of state-sponsored attacks started to backfire with large-scale consequences, undermining the security and stability of cyberspace for all users.

The private sector, academic actors, and other stakeholders who participate in Internet governance instances started to claim their own legitimacy and interest in taking part in the discussions over the security and stability of cyberspace. Academics created and built the Internet, later globalized and commercialized by the private sector. Most of the infrastructures are owned by major private companies that are at

[17] Markoff, M. G. (2017, June 23). *Explanation of Position at the Conclusion of the 2016–2017 UN Group of Governmental Experts (GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security*. https://usun.usmission.gov/explanation-of-position-at-the-conclusion-of-the-2016-2017-un-group-of-governmental-experts-gge-on-developments-in-the-field-of-information-and-tele/.

[18] Ibid.

[19] NETMundial Multistakeholder Statement, April 24, 2014. https://netmundial.br/wp-content/uploads/2014/04/NETmundial-Multistakeholder-Document.pdf.

https://doi.org/10.1017/9781108954341.009 Published online by Cambridge University Press

the forefront of the attacks, often playing the role of first defender. Because of their data, resources, and skills, they are an essential partner of states for their cybersecurity. Global technology companies also have a vested interest in the security and stability of cyberspace for the trust of their users and the performance of their products, which are under constant attack.

Microsoft Corporation is by far the most important private actor in cybersecurity policymaking efforts, and leads multiple initiatives to promote cyber norms. As early as 2015, the company called on states – then on private companies – to adopt new norms. Most importantly, in 2017, its president, Brad Smith, proposed a Geneva Digital Convention for states to commit to protecting civilians against state-sponsored attacks, and the creation of an international organization for the attribution of cyberattacks.[20] The reference to international humanitarian law indirectly acknowledged the representation of cyberspace as a warfighting domain, but put the emphasis on the risk borne by civilians. The propositions were, however, regarded as infringing on states' rights and privileges. They were also criticized for shifting all the responsibility on states while creating few constraints on the industry to secure its products, whose flaws are exploited by malicious actors to conduct offensive operations.

The company then shifted its focus to promote cyber peace through multiple initiatives: A public petition, a commitment for the industry (Cybersecurity Tech Accord[21]), and the launch of the Cyberpeace Institute,[22] in partnership with the Hewlett Foundation and Mastercard in 2019. Its missions are to promote transparency and accountability by investigating and analyzing cyberattacks that impact civilians, provide assistance to the most vulnerable victims of cyberattacks, and promote cybersecurity norms of responsible behavior. The keyword is accountability, reflecting an interest in emphasizing state responsibility for the lack of cybersecurity. Other private sector initiatives were launched, such as the Charter of Trust,[23] initiated by Siemens in 2018, which contains ten principles to increase the resilience of digital products and the integrity of the supply chain.

The deadlock among states prompted the creation, in February 2017, of the Global Commission on the Stability of Cyberspace (GCSC), a multistakeholder group of international experts coming from academia, civil society and technical organizations, government, and the private sector. The Commission, initiated by the Ministry of Foreign Affairs of the Netherlands, and supported by several governments, private companies, and public organizations, started its work "convinced that an issue traditionally reserved to states—international peace and security—could no longer be addressed without engaging other stakeholders."[24] During its three-year

[20] Smith, B. (2017, February 14). *The Need for a Digital Geneva Convention*. Microsoft. https://blogs.microsoft.com/on-the-issues/2017/02/14/need-digital-geneva-convention/.

[21] Cyber Tech Accord. https://cybertechaccord.org/.

[22] Cyber Peace Institute. https://cyberpeaceinstitute.org/.

[23] Charter of Trust. www.charteroftrust.com/.

[24] Global Commission on the Stability of Cyberspace. https://cyberstability.org/about/.

https://doi.org/10.1017/9781108954341.009 Published online by Cambridge University Press

mandate, its mission was to propose norms and initiatives to guide responsible state and nonstate behavior in cyberspace in order to enhance international peace and security, with a main focus on stability, defined as such in its final report:

> Stability of cyberspace means everyone can be reasonably confident in their ability to use cyberspace safely and securely, where the availability and integrity of services and information provided in and through cyberspace are generally assured where change is managed in relative peace, and where tensions are resolved in a non-escalatory manner.[25]

In November 2017, the Global Commission proposed a Call to Protect the Public Core of the Internet, and that proposition has since been included in the European Union Cyber Security Act. It released its final report at the Paris Peace Forum of 2018 and the Internet Governance Forum held at the same time in Paris.

On the same occasion, the president of France launched the Paris Call for Trust and Security in Cyberspace (Paris Call, 2018), an initiative strongly supported by Microsoft, which led to a commitment to a set of principles and norms of responsible behavior of over 1,100 signatories, including 79 states, as of March 2021 – but not Russia, China, or the United States. The Paris Call refers to five GCSC norms, making explicit reference to three of them.[26] This initiative also demonstrates how some states attempt to draw from the legitimacy of multistakeholder support in order to build consensus over norms of responsible behavior for states and industry in cyberspace. This was also the approach favored by the Secretary General of the United Nations when setting up a High-Level Panel on Digital Cooperation in July 2018 to "advance proposals to strengthen cooperation in the digital space among Governments, the private sector, civil society, international organisations, academia, the technical community and other relevant stakeholders."[27]

Although states widely recognize the role of the private sector in the security and stability of cyberspace, and many of them endorse the multistakeholder governance model, they also perceive cyberspace as an international security threat that should be addressed by international regulation, which is the sole prerogative of UN Member States. It is in a very tense geopolitical context, marked by large-scale devastating attacks, information warfare targeting democratic processes, and the weakening of multilateral institutions that, eventually, the OEWG and the sixth UN GGE were created.

[25] Global Commission on the Stability of Cyberspace. (2019). *Advancing Cyberstability: Final Report*, p. 13.

[26] The Paris Call for Trust and Security in Cyberspace includes references to the norm on the public core of the Internet (Principle 2), the norm on the protection of electoral infrastructures (Principle 3), and the norm on hack back (Principle 8).

[27] U.N. Secretary General. (June 2019). *The Age of Digital Interdependence, Report of the UN Secretary General's High-level Panel on Digital Cooperation*, p. 39. Digital Cooperation. https://digitalcooperation.org/wp-content/uploads/2019/06/DigitalCooperation-report-web-FINAL-1.pdf.

https://doi.org/10.1017/9781108954341.009 Published online by Cambridge University Press

2 THE CREATION OF TWO COMPETING PROCESSES AT THE UN: THE OPEN-ENDED WORKING GROUP AND THE SIXTH GROUP OF GOVERNMENTAL EXPERTS

2.1 *A Context of Heightened Strategic Competition*

The resolutions creating the OEWG and the GGE were introduced by two groups of states, one led by the Russian Federation, the other one by the United States, forming seemingly adversarial blocs. But the reality is more complex and nuanced.

Russia, supported by China and other states,[28] proposed a first draft resolution in October 2018 creating an OEWG. The draft resolution listed not only norms adopted by the GGE in 2015, but also norms taken from the International Code of Conduct for Information Security proposed by the member states of the Shanghai Cooperation Organization in 2015 – and rejected by Western governments. In response, the United States submitted an alternative draft for a resolution creating a sixth GGE, which was supported by many European countries.[29] Eventually, Russia and cosponsoring states modified their project to account for the many criticisms they had received. But the United States and their cosponsors did not retract their own draft, arguing that the revised Russian draft still contained unacceptable provisions and did not reflect the 2015 GGE final report as well as it claimed. As a result, two competing resolutions on ICTs in the context of international security were debated in the First Committee of the UNGA; one promoted by Russia, the other by the United States. Both were adopted within a few days of each other, to the surprise of a number of states.

Heightened tensions between states surrounded the debates. According to the press communiqué describing the debates, Iran "[a]s a victim of cyber weapons," supported the "establishment of international legal norms and rules aimed at preventing the malicious use of cyberspace and information and communications technology" and condemned "those seeking dominance and superiority in cyberspace and their attempts to maintain the status quo" and pointed to a certain state (the United States) which, "in collaboration with Israel, used the computer worm

[28] Algeria, Angola, Azerbaijan, Belarus, Bolivia, Burundi, Cambodia, China, Cuba, Eritrea, the Russian Federation, Kazakhstan, Madagascar, Malawi, Namibia, Nepal, Nicaragua, Uzbekistan, Pakistan, the Syrian Arab Republic, the Democratic Republic of Congo, Samoa, Sierra Leone, Surinam, Tajikistan, Turkmenistan, Venezuela, and Zimbabwe. UNGA: *Developments in the field of information and telecommunications in the context of international security*, A/C.1/73/L.27/Rev.1 (2018).

[29] Germany, Australia, Austria, Belgium, Bulgaria, Canada, Croatia, Cyprus, the Czech Republic, Denmark, Estonia, Finland, France, Georgia, Greece, Hungary, Ireland, Israel, Italy, Japan, Latvia, Lithuania, Luxembourg, Malawi, Malta, the Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Ukraine, the United Kingdom, and the United States of America. UNGA: *Advancing responsible State behavior in cyberspace in the context of international security*, A/C.1/73/L.37 (2018).

https://doi.org/10.1017/9781108954341.009 Published online by Cambridge University Press

Stuxnet against Iran's critical infrastructure, and yet has tabled a draft resolution regarding responsible state behaviour in cyberspace."[30]

The representative of China asked whether a negative vote on the Russian resolution would bring a "ticket" for the country to take part in the GGE, knowing that the number of participants is limited to twenty-five states, including the five permanent members of the UN Security Council.[31]

The debates gave the impression of two competing blocs of states, sponsoring different resolutions initiated by two states with diametrically opposed approaches on how to regulate cyberspace and what the content of the negotiations should be: On the one side, the United States and European countries, usually described as the "like-minded state," and on the other side, China and Russia. However, greater nuance is needed both in the homogeneity of the two blocs of states and the antagonism underlying their respective positions.

First, the countries in each group are not really homogeneous, they share certain characteristics in their approach that are not completely alike. There are, for example, important divergences between the Chinese approach and the Russian one,[32] as well as between France and the United States.

Second, the majority of UN member states did not adhere to any of the two groups and felt caught in the middle without a full grasp of the stakes. This supports an argument for the idea of two poles instead of two blocs of states structuring in international negotiations. More importantly, the vast majority of the member states voted in favor of both resolutions, as they regarded them as potentially complementary.[33] While these two processes might effectively be competing, they each advanced different sets of interests. The OEWG is open to all the member states, taking all the points of view into account. But, on the contrary, the composition of the GGE is limited to twenty-five member states designated "on the basis of equitable geographical distribution,"[34] the permanent members of the Security Council being *ex officio* members. Hence, the GGE appears as a more specialized entity

[30] Meetings Coverage, UNGA, First Committee Delegates Exchange Views on Best Tools for Shielding Cyberspace from Global Security Threats Triggered by Dual-Use Technologies, GA/DIS/3613 (Oct. 30, 2018).

[31] Meetings Coverage, "First Committee Approves 27 Texts, Including 2 Proposing New Groups to Develop Rules for States on Responsible Cyberspace Conduct, Meetings Coverage," GA/DIS/3619 (Nov. 8, 2018).

[32] Broeders, D., Adamson, L. & Creemers, R. (2019, November 5). A *Coalition of the Unwilling? Chinese and Russian Perspectives on Cyberspace*. Universiteit Lieden. www.universiteitleiden.nl/en/research/research-output/governance-and-global-affairs/a-coalition-of-the-unwilling-chinese-and-russian-perspectives-on-cyberspace.

[33] The resolution "Developments in the field of information and telecommunications in the context of international security" (UNGA Res. 73/27 (Dec. 5, 2018)) was adopted with 119 votes against 46 and 14 abstentions (UNGA A/73/PV.45 (2018)) and the resolution "Advancing responsible State behaviour in cyberspace in the context of international security" (UNGA Res. 73/266 (Dec. 22, 2018)) was adopted with 138 votes against 12 and 16 abstentions (UNGA A/73/PV.65 (2018).

[34] UNGA Res. 73/266, ¶ 3 (Jan. 2, 2019).

https://doi.org/10.1017/9781108954341.009 Published online by Cambridge University Press

which could lead to concrete progress on the core questions debated, whereas the nonlimited composition of the OEWG offers a more inclusive approach that allows each state to have its positions and interests heard.

The first session of the OEWG, which took place in New York in September 2019, actually highlighted the interests that many states have in taking an active part in the discussions – something confirmed by the high number of states involved in the second formal session in February 2020, as observed through the online videos of the debates on the UN website. Hence, the two ongoing processes are somewhat complementary. Despite the hostile climate that surrounded their creation, which reveal strong geopolitical tensions, they offer – in theory at least – a possibility for states to go beyond their inherent divisions and offer a smooth parallel functioning, or even synergy. The ambassadors Guilherme de Aguiar Patriota and Jürg Lauber, who preside over the GGE and the OEWG, respectively, actually advertised this constructive ambition from the moment they were nominated in these roles, as they have publicly declared on multiple occasions.

The complementarity of the two cyber norms processes has been highlighted by several states. However, an analysis of their respective mandates shows that, if they can be complementary, their mandates overlap to a certain extent, which does not facilitate the search for consensus and coherence in the negotiations.

2.2 *Overlapping Mandates and Subtle Differences*

At first glance, the mandates of the two groups are so similar they overlap to a large extent, with the risk of encroaching on one another. Indeed, both groups are mandated to work on the norms, rules, and principles of responsible behavior of the states, on confidence building measures, on capacity building, and international law. However, a careful reading reveals several differences.

First, the GGE can consult states that are not part of the GGE and competent regional organizations such as the African Union, the Organization of American States, the Organization for Security and Co-operation in Europe, and the Regional Forum of the Association of Southeast Asian Nations. The OEWG, on the other hand, is empowered to hold informal sessions to consult private actors and non-governmental organizations. Furthermore, nonstate actors are authorized to attend the formal sessions as long as they have an accreditation with the United Nations Economic and Social Council (ECOSOC), following the Chinese refusal to further enlarge the pool.

Second, the GGE report is to be presented to the General Assembly with "an annex containing national contributions of participating governmental experts on the subject of how international law applies to the use of information and communications technologies by states."[35] As such, the twenty-five countries participating

[35] UNGA Res. 73/266, ¶ 3 (Jan. 2, 2019).

https://doi.org/10.1017/9781108954341.009 Published online by Cambridge University Press

in the GGE will have to clarify their position on the international law applicable to cyber operations. Some states, such as France and the Netherlands, have already moved forward in this regard. The French Ministry of Armed Forces published a report, *International Law Applied to Cyberoperations*,[36] in 2019, and the Dutch Ministry of Foreign Affairs also published *International Law in Cyberspace* in 2019.[37] These documents are most likely meant to be the two countries' national contributions to the GGE.[38]

Finally, the OEWG is tasked with examining "the possibility of establishing regular institutional dialogue with broad participation under the auspices of the United Nations"[39] to deal with ICTs in the context of international security. It could take the form of a permanent body or a new process.

A number of differences have raised concerns, starting with the respective timelines. The OEWG was supposed to end its work in 2020 and submit its report to the UNGA during its 75th session, a year before the GGE. Indeed, the GGE's mandate ends in May 2021 and the GGE should thus present its report to the UNGA during its 76th session. The extension of the 75th session until March 2021, due to the COVID-19 crisis, allowed the OEWG's work to continue in order to present it to the 76th session of the UNGA. The final deadlines for the two reports have therefore been preserved. Yet, some observers worry that several states behind the resolution creating the OEWG might change course after the end of its sessions. In other words, they would be adopting a constructive approach up to the end of the OEWG's work in order to achieve a consensus on its conclusions, before becoming less cooperative during the remaining time of the GGE sessions to push for a failure, and boast of the superior achievements of the OEWG. But given the short time between the end of the two processes, this might be more difficult to achieve.

The second concern regards the content of the mandates. Both processes discuss international law, which constitutes a central topic in their proceedings. This can be seen both as an opportunity and a risk: States may conduct meaningful discussions and make progress on a consensus about the interpretation of international law in this new context of international peace and security, but they also may take

[36] France, Ministry of Armed Forces. (2019, September 9). *International law applied to cyberoperations*. www.defense.gouv.fr/content/download/565895/9750877/file/Droit+internat+appliqu%C3%A9+aux+op%C3%A9rations+Cyberespace.pdf.

[37] Netherlands (made public on September 26, 2019). *Letter of July 5, 2019 from the Minister of Foreign Affairs to the President of the House of Representatives on the international legal order in cyberspace*. Annex. www.government.nl/documents/parliamentary-documents/2019/09/26/letter-to-the-parliament-on-the-international-legal-order-in-cyberspace.

[38] For a compared study of the states' positions on international law applied to cyberoperations, see Roguski, P. (2020). *Application of International Law to Cyber Operations: A Comparative Analysis of States' Views*. The Hague Program on Cyber Norms. www.thehaguecybernorms.nl/research-and-publication-posts/application-of-international-law-to-cyber-operations-a-comparative-analysis-of-states-views.

[39] UNGA Res. /27, ¶ 5 (Dec. 5, 2019).

https://doi.org/10.1017/9781108954341.009 Published online by Cambridge University Press

diverging directions in the two processes, leading to a certain level of instability for the international legal order.

This concern also applies to norms of responsible state behavior, mentioned twice in resolution 73/27 that defines the mandate of the OEWG. The situation here is delicate for two reasons. The first mention of norms in resolution 73/27 appears early on in the definition of the OEWG mandate in paragraph 5.[40] Norms – as stated in the resolution – constitute the working base of the OEWG, but their definition is slightly different from the norms of the 2015 GGE report to which they refer. The mandate of the GGE is clearer since resolution 73/266 refers exclusively to the GGE report. As a result, the working base of the two processes could slightly differ and potentially increase the risks of divergence, or even contradiction in the meaning of the recommendations adopted by each process. For example, the recommendation on the prevention of malicious computer tools or technologies is included in a paragraph on supply chain integrity in the 2015 GGE report, whereas it is the subject of a stand-alone provision in resolution 73/27 that creates the OEWG. This could indicate a desire to work more extensively on the issue of proliferation in the context of the OEWG.

The practice of the states, however, shows that this risk remains limited as a large majority of states, during the first two sessions of the OEWG, opted for the norms as stated in the 2015 GGE report. This illustrates the lack of consensus on the norms as stated in the provisions of resolution 73/27, but it also highlights a gap between a strict application of the mandate and the practice adopted by states during the negotiations.

The uncertainty around the working base could also affect other aspects of the negotiations, such as norm implementation.[41] Member states are tasked with detailing the operationalization of the norms. Because several of them are quite vague, they need to be specified in order to be implemented. Finally, the OEWG mandate paves the way for a possible reappraisal of the agreed provisions of the 2013 and 2015 GGEs as states are able to "introduce changes,"[42] including establishing new norms. Elaborating new norms is authorized by resolution 73/27 and could involve creating new norms that better define what responsible behavior is, or revisit the norms adopted in the 2013 and 2015 reports.

The second mention of norms in the resolution 73/27 can be found in the second part of the definition of the mandate. But it does not state explicitly if this mention refers to the norms stated in resolution 73/27 or the ones adopted by the GGEs in 2013 and 2015.

[40] "[A]cting on a consensus basis, to continue, as a priority, to further develop the rules, norms and principles of responsible behaviour of states listed in paragraph 1 above, and the ways for their implementation; if necessary, to introduce changes to them or elaborate additional rules of behaviour." UNGA Res. /27, ¶ 5 (Dec. 5, 2019).

[41] UNGA Res. 73/27, ¶ 5 (Dec. 5, 2019).

[42] Ibid.

https://doi.org/10.1017/9781108954341.009 Published online by Cambridge University Press

A close reading of the mandate thus highlights a number of questions related to the working base on which the negotiations are to be conducted. The practice of using the GGE norms have prevailed so far, but contradictions could emerge as both the GGE and the OEWG are tasked with working on these provisions.

It was also hard to know how the work would be divided between the two processes, given the fact that international law and norms of responsible behavior are mentioned in both mandates. In his speech during the first session of the OEWG in June 2019, the special representative of the President of the Russian Federation for international cooperation in information security proposed that the OEWG deals with norms of responsible behavior, confidence building measures, and measures of international cooperation and assistance, hence leaving the issue of international law to the GGE.[43] This proposal was not accepted. As a result, both processes work concomitantly on the entire set of issues.

This situation is both understandable and problematic. On the one hand, international laws and norms of responsible state behavior are intrinsically linked and, therefore, difficult to completely dissociate. On the other hand, this situation reinforces the risk of repetitions in the content of the negotiations, and also the risk of contradictions in the recommendations made by the two groups on the rights and obligations of states. Most importantly, the refusal to dissociate them highlights disagreements on the necessary means to ensure security and stability of cyberspace.

The COVID-19 pandemic has added a layer of complexity. In addition to overlapping mandates, the two processes have ended up with largely overlapping calendars since the two final reports will be produced a month apart from each other. It is, however, difficult to assess whether this overlapping can help build synergy between the two processes or fuel further rivalry. Most importantly, states have not waited for the end of these two processes, as initially planned, to propose new processes.

3 BUMPY ROAD TO CYBER PEACE

3.1 *New Path(s) for Cyber Stability?*

In the face of potential difficulties in reaching consensus over a final report and successfully coordinating the two existing processes, France and Egypt, supported by thirty-eight countries and the European Union, proposed on October 1, 2020, a new path to cyber stability: The creation of a Program of Action (PoA) for advancing responsible state behavior in cyberspace, a proposal made to all member states

[43] Embassy of the Russian Federation to the United Kingdom of Great Britain and Northern Ireland (June 7, 2019). *Statement by Amb. Andrey Krutskikh, Special Representative of the President of the Russian Federation for International Cooperation in the Field of Information Security at the First Session of the UN Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security, New York, 3–4 June 2019*. https://rusemb.org.uk/article/541.

https://doi.org/10.1017/9781108954341.009 Published online by Cambridge University Press

within the context of the OEWG. Neither China, Russia, nor the United States have been officially part of this initiative.

A PoA consists of the production of an outcome document adopted by an intergovernmental conference, considered as politically binding, which contains objectives, recommendations, and rules for implementation and monitoring, in a new process with working conferences every other year including a review conference every five years.[44] It would, therefore, fulfill one of the objectives of the OEWG; that is, "study the possibility of establishing a regular institutional dialogue with broad participation under the auspices of the United Nations."[45]

This process would present the advantage of bringing the discussion back into a single process more inclusive than the GGE. As a new process, it would also be free from all the political baggage linked to the United States versus Russia rivalry over the GGE and OEWG processes. Unlike previous dialogues, it would not require building a consensus over a final report but, rather, building a working relationship that fosters practical cooperation and allows for agreement on specific issues as the discussions progress. There would be no end dates, even if states fail to agree on an outcome document at the end of a technical or review conference. The ultimate goal is to preserve and build on the agreed provisions of the previous GGE by providing a "forum for practical cooperation and ongoing discussions."[46]

Although the proposition was well received, two draft resolutions were put forward before the UNGA First Committee a few days later.[47] On October 5, a coalition of forty-six member states led by the United States, including France and many supporters of the PoA, proposed a draft resolution entitled "Advancing responsible state behaviour in cyberspace in the context of international security." The resolution acknowledges the ongoing discussions at the GGE and OEWG and declares that member states will study the conclusions of both groups and "will decide thereafter on any future work, as needed."[48]

The very next day, jumping ahead of the calendar, Russia along with fourteen other states proposed another draft resolution stating – in operative paragraph 1 – that the UNGA will create a new OEWG starting in 2021, without waiting for the conclusions of the two ongoing processes.[49] A revised version was submitted

[44] Delerue, F. & Géry, A. (2020, October 6). *A New UN Path to Cyber Stability*. Directions Blog. https://directionsblog.eu/a-new-un-path-to-cyber-stability/.

[45] UNGA Res. 73/27, ¶ 5 (2018).

[46] Australia. (2020, December 2). *Informal Australian Research Paper: What Next for Advancing Responsible State Behaviour at the United Nations*. https://front.un-arm.org/wp-content/uploads/2020/12/australian-research-paper-revised-december-2020-version-2-oewg-regular-institutional-dialogue.pdf.

[47] UNGA, *Developments in the field of information and telecommunications in the context of international security*. Report of the First Committee, A/75/394 (2020).

[48] UNGA, *Advancing responsible state behavior in cyberspace in the context of international security*, A/C.1/75/L.4 (2020).

[49] UNGA, *Establishment of a nuclear-weapon-free zone in the region of the Middle East*, A/C.1/75/L.8 (2020).

https://doi.org/10.1017/9781108954341.009 Published online by Cambridge University Press

on October 26, specifying that the new OEWG "shall start its activities up to the conclusion of the work of the current Open-Ended Working Group and considering its outcomes."[50] The revised version, however, leaves room for interpretation as to whether the acquis will be preserved, since the mandate of the new OEWG includes the possibility to "if necessary, … introduce changes to them [the norms] or elaborate additional rules of behaviour."[51] In addition, this new draft resolution borrows from the PoA approach by stating that the new OEWG "may decide to establish thematic subgroups, as the Member States deem necessary, with a view to fulfilling its mandate and facilitating the exchange of views among States on specific issues related to its mandate, and may decide to interact, as appropriate, with other interested parties, including businesses, non-governmental organizations and academia."[52] Yet, while it opens the door to consultations with nonstate actors, the drafting is less prescriptive than in the resolution that created the first OEWG, and it will limit nonstate actors' participation in the discussions for the next five years. And, finally, there is a tweak that leaves the question of its future mandate open: The name changed from "OEWG on developments in the field of information and telecommunications in the context of international security" to "OEWG on security of and in the use of information and communication technologies."[53]

Both draft resolutions were submitted to a vote at the First Committee on November 9, 2020, and both were adopted. The UNGA adopted both of them respectively on December 7th (UNGA Res. 75/32 (2020)) and December 31st (UNGA Res. 75/240 (2020)), adding more confusion to the field of competing processes. The PoA was proposed to all participating states during the discussions held within the OEWG, and offered to continue the negotiations within a single process. The resolution sponsored by Russia offered to continue this dialogue within the OEWG and the resolution sponsored by the United States suggested to wait and see. These competing initiatives have fostered strong debates within the United Nations and, more broadly, among actors involved on these matters.

3.2 *The Contest for Normative Influence*

Once again, the debates seemed to oppose two blocs, one led by the Russian Federation and the other by Western states along with Australia, even though the reality was more complex. We studied the coalition of sponsors and the votes at the UNGA for each resolution. The analysis reveals that the United States gained support among states since its 2018 resolution, while Russia has lost part of its support (Figure 9.1).

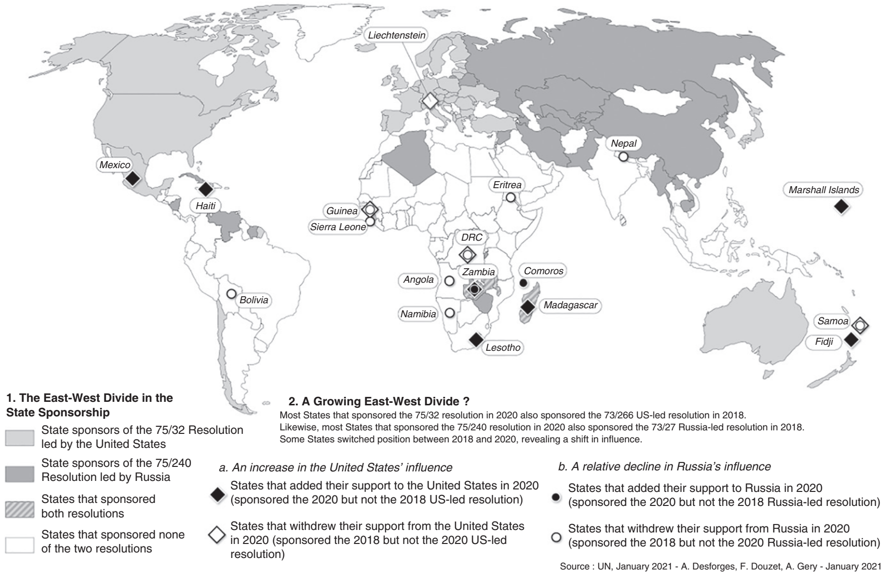
[50] UNGA, *Developments in the field of information and telecommunications in the context of international security*, A/C.1/75/L.8/Rev.1 (2020).

[51] Ibid., ¶ 1.

[52] Ibid., ¶ 4.

[53] Ibid., op. ¶ 4.

https://doi.org/10.1017/9781108954341.009 Published online by Cambridge University Press


Liechtenstein
Nepal
Mexico
Haiti
Eritrea
Marshall Islands
Guinea
Sierra Leone
DRC
Zambia
Comoros
Angola
Bolivia
Madagascar
Namibia
Samoa
Fidji
Lesotho
1. The East-West Divide in the State Sponsorship
State sponsors of the 75/32 Resolution led by the United States
State sponsors of the 75/240 Resolution led by Russia
States that sponsored both resolutions
States that sponsored none of the two resolutions
2. A Growing East-West Divide ?
Most States that sponsored the 75/32 resolution in 2020 also sponsored the 73/266 US-led resolution in 2018.
Likewise, most States that sponsored the 75/240 resolution in 2020 also sponsored the 73/27 Russia-led resolution in 2018.
Some States switched position between 2018 and 2020, revealing a shift in influence.
a. An increase in the United States' influence
States that added their support to the United States in 2020 (sponsored the 2020 but not the 2018 US-led resolution)
States that withdrew their support from the United States in 2020 (sponsored the 2018 but not the 2020 US-led resolution)
b. A relative decline in Russia's influence
States that added their support to Russia in 2020 (sponsored the 2020 but not the 2018 Russia-led resolution)
States that withdrew their support from Russia in 2020 (sponsored the 2018 but not the 2020 Russia-led resolution)

Source : UN, January 2021 - A. Desforges, F. Douzet, A. Gery - January 2021

FIGURE 9.1 State sponsorship of 2020 UN Cyber Diplomacy Resolutions: a persistent east-west divide.

The map "State Sponsorship of 2020 UN Cyber Diplomacy Resolutions" illustrates a clear east-west divide regarding the sponsorship of the two resolutions. The US-led resolution 75/32 was overwhelmingly supported by Western countries while the Russian led resolution 75/240 was supported by Eastern Countries. But the map also reveals a slight change of balance in favor of the United States. In 2020, eight states that had sponsored the Russian-led resolution in 2018 withdrew their support to Russia for the 2020 resolution. In the meantime, two states (Comoros and Zambia) added their support to Russia; that is, sponsored the 2020 resolution but not the 2018. But Zambia also sponsored the US-led resolution. On the contrary, the US-led resolution gained sponsorship between 2018 and 2020: Seven states added their support to the United States in 2020 while four withdrew their support, as illustrated by the graph in Figure 9.2.

The two draft resolutions were introduced before the UN First Committee on the October 5–6, 2020. The first one, "Advancing responsible State behaviour in cyberspace in the context of international security,"[54] was introduced by the United States on behalf of fifty-three states, against fifty-one states for the 2018 US-sponsored resolution.[55] The vote at the First Committee reached a large

[54] UNGA, *Advancing responsible State behavior in cyberspace in the context of international security*, A/C.1/75/L.4 (2020).

[55] UNGA, *Developments in the field of information and telecommunications in the context of international security*. Report of the First Committee, A/73/505 (2018).

https://doi.org/10.1017/9781108954341.009 Published online by Cambridge University Press

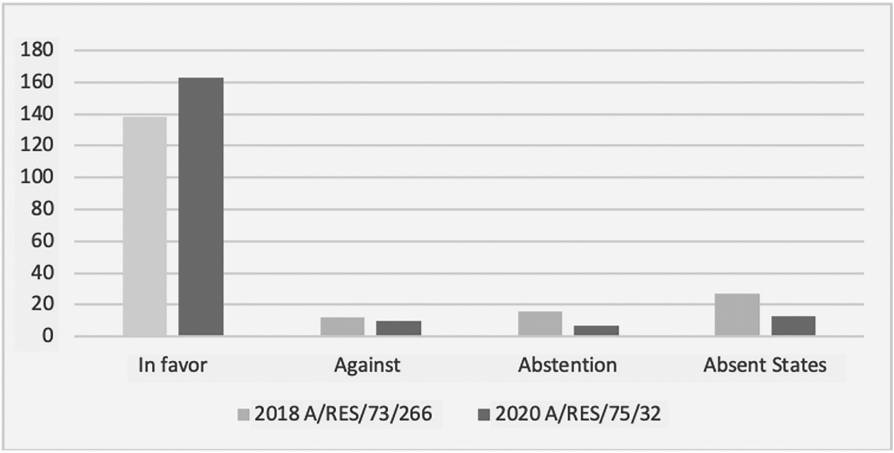


FIGURE 9.2 The 2020 US-led resolution gains more votes than the 2018 resolution.

consensus with 153 states in favor, 9 against, and 9 abstaining. The UNGA adopted the resolution in its plenary session on December 7, 2020, by an even larger margin: 163 in favor, 10 against, and 7 abstaining. By comparison, the 2018 US-sponsored resolution was adopted by a lower margin (138 in favor, 12 against, 9 abstaining). This can be explained by the noncontentious nature of the 2020 resolution, which did not involve a strong commitment to a specific process.

The draft resolution A/C.1/75/L.8/Rev.1, sponsored by Russia on behalf of twenty-six states (thirty-four in 2018), however, was faced with harsh criticism coming mainly from Western states. The representative of the Russian Federation, speaking in exercise of the right of reply, said: "Western delegations are sabotaging the process and breaking with decades of consensus on cybersecurity." As such, his delegation was offended by their level of cynicism and hypocrisy, which stalled the work of the OEWG. He added, "If it were not for the Russian Federation, the United Nations would not have open negotiations on the matter."[56]

The opposition focused on operative paragraph 1, creating a new OEWG for 2021. Western states objected that it is part of the mandate of the present OEWG to make suggestions about future institutional work and, therefore, decide whether a new OEWG should be created. The draft resolution would thus preempt the work

[56] Meeting's coverage, UNGA (2020, November 9), First Committee Approves 15 Draft Resolutions, Decisions on Disarmament Measures, Including 2 Following Different Paths towards Keeping Cyberspace Safe, GA/DIS/3659 (Nov. 9, 2020).

https://doi.org/10.1017/9781108954341.009 Published online by Cambridge University Press

of the present OEWG. They therefore asked for the withdrawal of this operative paragraph and all related ones.

The Russian delegates strongly opposed this demand; they believed that this would void the resolution of all substance and invoked article 129 of the Rules of Procedures of the UNGA[57] to have the contentious operative paragraph 1 be voted on separately instead of withdrawn. This situation in itself illustrates the opposition between Western states and the Russian Federation. As a result, the President of the First Committee put to a vote the decision regarding the division of the draft resolution, which was approved by fifty-seven states in favor, thirty-one against, and sixty-three abstaining. Once the division approved, the First Committee then proceeded to the three following votes on: the preamble (108 in favor, 49 against, 11 abstaining); the operative paragraph 1 (92 in favor, 52 against, 24 abstaining); and the resolution as a whole (104 in favor, 50 against, 20 abstaining).

The resolution was thus submitted to the UNGA and adopted on December 31, 2020. The date in the middle of the holiday season may explain the high number of absent states on the day of the vote. The voting data show an overall support for the resolution and also a sizeable opposition: ninety-two in favor, fifty against, and twenty-one abstaining. The Russia sponsored resolution was nevertheless adopted by the UNGA, yet the number of States voting in favor (92) was drastically lower than for the 2018 Russia sponsored resolution (119 in favor). However, this result must be interpreted with caution. Thirty states were absent from the UNGA that day, among which eighteen states who voted in favor of the Russia sponsored resolution in 2018. A close reading of the votes shows, however, that Russia indeed lost the support of an additional thirteen member states compared to 2018, as illustrated by the graph in Figure 9.3.

The charts "The 2020 UNGA Balance of Votes" illustrate the percentage of states that voted in favor of each resolution, against it, or abstained (Figure 9.4).

The map "UNGA Vote on 2020 Cyber Diplomacy Resolutions," with the votes on the two resolutions, highlights the dynamics of power between states. First, it confirms the East-West divide observed on the state sponsorship map. It also confirms the growing support gained by the United States, whose resolution was adopted by a larger and growing margin of states (with fewer absent states) and by less opposition. In addition, support for the US-led resolution appeared more consistent. All the states that had only sponsored the US-led resolution in 2020 voted for it and, in

[57] *"A representative may move that parts of a proposal or of an amendment should be voted on separately. If objection is made to the request for division, the motion for division shall be voted upon. Permission to speak on the motion for division shall be given only to two speakers in favour and two speakers against. If the motion for division is carried, those parts of the proposal or of the amendment which are approved shall then be put to the vote as a whole. If all operative parts of the proposal or of the amendment have been rejected, the proposal or the amendment shall be considered to have been rejected as a whole."*

https://doi.org/10.1017/9781108954341.009 Published online by Cambridge University Press

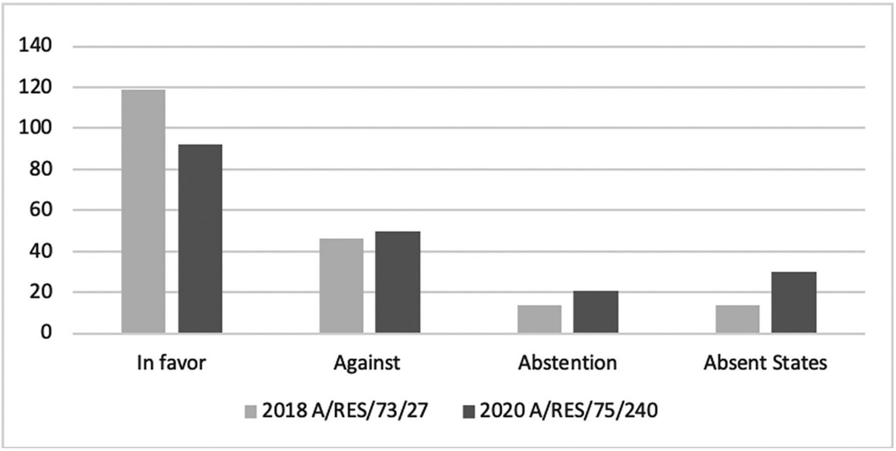


FIGURE 9.3 The 2020 Russian-led resolution gathers less votes than the 2018 resolution.

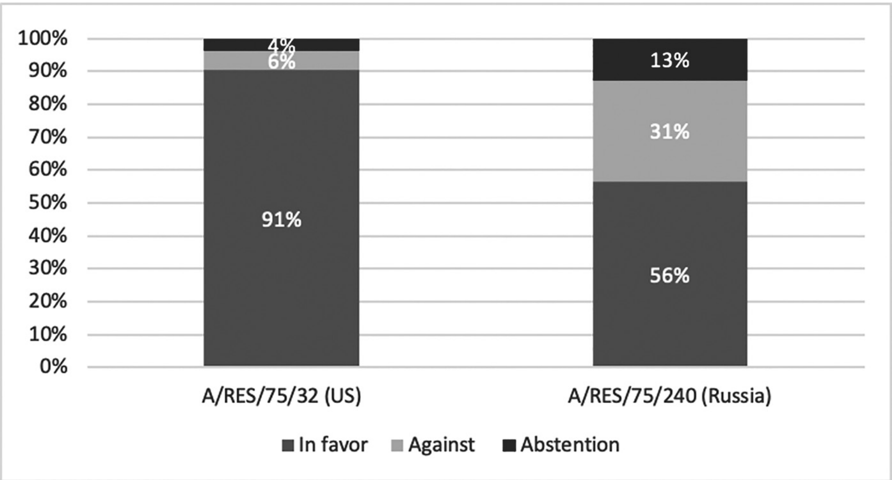
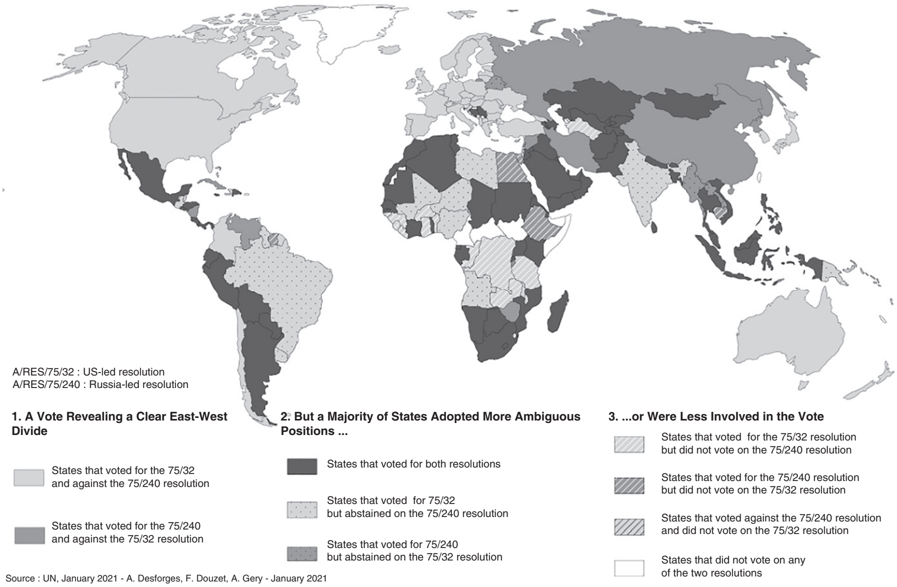


FIGURE 9.4 The 2020 UNGA balance of votes.

addition, voted against the Russia-led resolution (none of them abstained or voted in favor of it) (Figure 9.5).

On the contrary, several states that had sponsored the Russia-led resolution did not oppose the US-led resolution: They either voted in favor of it or abstained. This could be explained by the fact that the US-led resolution is more consensual than the Russia-led resolution, but it also reveals a more complex picture. A majority of states either voted for both resolutions or voted for one and abstained from

https://doi.org/10.1017/9781108954341.009 Published online by Cambridge University Press


A/RES/75/32 : US-led resolution
A/RES/75/240 : Russia-led resolution
1. A Vote Revealing a Clear East-West Divide
States that voted for the 75/32 and against the 75/240 resolution
States that voted for the 75/240 and against the 75/32 resolution
2. But a Majority of States Adopted More Ambiguous Positions ...
States that voted for both resolutions
States that voted for 75/32 but abstained on the 75/240 resolution
States that voted for 75/240 but abstained on the 75/32 resolution
3. ...or Were Less Involved in the Vote
States that voted for the 75/32 resolution but did not vote on the 75/240 resolution
States that voted for the 75/240 resolution but did not vote on the 75/32 resolution
States that voted against the 75/240 resolution and did not vote on the 75/32 resolution
States that did not vote on any of the two resolutions

Source : UN, January 2021 - A. Desforges, F. Douzet, A. Gery - January 2021

FIGURE 9.5 UNGA vote on 2020 Cyber Diplomacy Resolutions: a majority of states caught between two stools.

the other. This shows that the East-West divide is clear, but most states – caught between two stools – chose not to position themselves within this duopoly. Any claim that international negotiations on the security and stability of cyberspace is marked by a strong opposition between two blocks of states should thus be cautioned.

CONCLUSION

The cyber peace building dynamics at the United Nations reflects fundamental disagreements on the means to ensure the security and stability of cyberspace and the struggle for normative influence among states.

Russia has justified its 2020 initiative by the desire to ensure that international discussions would continue after the end of the two processes, highlighting its role in opening negotiations. But the Russian Federation might also be defending another agenda, along with its own legal culture and perspective. Russia makes no secret of wanting to elaborate a treaty for cyberspace, an option best preserved by the OEWG process. A PoA, on the contrary, could considerably delay the perspective of a treaty by providing a process with no end date and “politically binding” decisions, a compromise that is *a priori* at odds with Russia’s legalist approach to international relations. Yet, Russia could also use the PoA as a vehicle to launch the drafting process of a treaty.

https://doi.org/10.1017/9781108954341.009 Published online by Cambridge University Press

The analysis of the maps shows there is a strong polarization between the United States and Russia and a relative decline in Russia's influence. However, Russia's leadership is still strong enough to get its resolution voted by the UNGA and there is still a vast reserve of votes, given the ambiguous position of a significant number of states. Indeed, a majority of states did vote for both resolutions, or chose to vote for one resolution without opposing the other.

To the surprise of all observers, states participating in the OEWG were able to reach a consensus and adopt a report on March 12, 2021,[58] while the GGE had still not ended its mandate. Meanwhile, a new OEWG is scheduled to start its work soon after the adoption of the consensus report since the UNGA enacted its creation in resolution 75/240. This leaves the question of the creation of other processes totally open, particularly since the PoA proposal has been acknowledged by the OEWG. Indeed, the final report recommended that "the Programme of Action should be further elaborated including at the Open-Ended Working Group process established pursuant to General Assembly resolution 75/240."[59] Although the report states that the PoA should be discussed within the future OEWG, it also leaves room for discussion of a PoA in another context. In this regard, the French Ambassador for Digital Affairs, Henri Verdier, announced on March 24, 2021 that France was considering launching the PoA in October 2021[60]; that is, at the beginning of the 76th session of the UN General Assembly. If this was to happen, it would raise the question of how many processes could states handle without ending in a total deadlock, letting alone the fact that another GGE could also be created in the meantime. While the PoA could offer a productive venue for states that wish to work on more action-oriented recommendations, it could also lead to more bumps in the road to cyber peace.

The road to cyber peace is arduous, given the will of states to preserve their ability to conduct cyber offensive operations. Official documents tend to refer to cyber stability rather than cyber peace as a goal for international negotiations.[61] The proliferation of damaging attacks and the risk of conflict escalation in cyberspace have led states to leverage the traditional instruments of collective security – such as international law and nonbinding norms of responsible behavior – to regulate cyberspace. In the early stages of consensus building up

[58] UNGA, *Final report of the OEWG*, A/AC.290/2021/CRP.2 (2021).

[59] Ibid., ¶ 77.

[60] Statement of the French Ambassador for Digital Affairs Henri Verdier at the launching meeting of the working group 3 of the Paris Call for Trust and Security in Cyberspace (March 24, 2021).

[61] The Global Commission has given its own definition of Stability of Cyberspace: "Stability of cyberspace means everyone can be reasonably confident in their ability to use cyberspace safely and securely, where the availability and integrity of services and information provided in and through cyberspace are generally assured, where change is managed in relative peace, and where tensions are resolved in a non-escalatory manner." Global Commission on the Stability of Cyberspace. (2019). *Advancing Cyberstability: Final Report*, p. 13.

https://doi.org/10.1017/9781108954341.009 Published online by Cambridge University Press

to 2016, these instruments have helped advance the discussions by providing an existing legal framework applicable to cyber operations as a basis for negotiation. But since then, the renewed strategic competition and exacerbated geopolitical tensions have led states to engage not only in a cyber arms race, but also in a competition for normative influence. As a result, international law has proved to be exactly what it is: An instrument in the service of state foreign policy – with the risk to lead states to a stalemate.

https://doi.org/10.1017/9781108954341.009 Published online by Cambridge University Press

https://doi.org/10.1017/9781108954341.009 Published online by Cambridge University Press