KONRAD ADENAUER STIFTUNG

MULTILATERALISM AND THE RISING CHALLENGES OF GLOBAL CYBER INSECURITY

By Eleonore Pauwels

JANUARY 2022

Cover photo: © NicoElNino / iStock / Getty Images Plus

Table of Content

Preface

Information and Communication Technologies (ICT) are not only reshaping our economies and societies, they impact and redefine international relations and international security. Over the last two decades, cyber threats and the malicious use of ICTs by State and Non-State actors have endangered supply chains, essential public services, and have added new dimensions of warfare. Due to its global scope and transboundary character, cybersecurity became a crucial topic on the agenda of multilateral institutions such as the United Nations (UN).

Although a specific and binding legal framework for regulating cyber security in the form of a treaty still remains out of reach, the UN can play a vital role in identifying existing and emerging threats, through confidence building measures as well as through capacity building for its Member States. The Governmental Group of Experts (GGE) which consists today of 25 experts from UN Member States has since its inception in 2004 contributed to the discussion on how international law applies in the use of ICTs, and what kind of norms, rules and principles guide responsible behavior of States.

In addition to the GGE and for the first time, an Open-Ended Working Group (OEWG) was established in 2019. Its multi-stakeholder approach moved the topic of cyber security out of the exclusivity of intergovernmental relations and allowed all Member States, private sector, academia and civil society to engage equally on the topic.

Both tracks, working in parallel in the period 2019-2021 have identified matters of concern that need to be addressed by Member States and where the UN has to take a lead if it aims to stay relevant as a catalyst for normative leadership and governance in a rapidly changing world.

In order to raise awareness and to bring the work and the recommendations of the GGE and the OEWG closer to political decision-makers on Member State level, the office of Konrad-Adenauer-Stiftung at the United Nations in New York has commissioned the present analysis by Eleonore Pauwels, a renowned International Expert in Converging Technologies and a Senior Fellow with the Global Center on Cooperative Security.

We wish you an interesting read!

Andrea E. Ostheimer
KAS Representative to the United Nations, New York

KONRAD ADENAUER STIFTUNG

Executive Summary

This paper aims to analyse the 2021 achievements of the UN Groups in the Field of Information and Telecommunications in the Context of International Security – the Open-Ended Working Group (OEWG) and the UN Governmental Group of Experts (GGE). Both have concluded their current missions in March and May 2021, respectively, and published their final reports.[1]

Section 1 provides a comparative analysis of the principal discussion results, challenges faced and progress made by the OEWG and the Sixth GGE. It sheds light on salient tensions and dynamics between member states in the GGE and the OEWG, as well as, in the latter, important and consequential interactions with civil society and the private sector. It also investigates to what extent complementarity between both groups has been achieved. Section 2 provides a unique assessment of the evolving cyberthreats landscape, including a comparison of how those threats are framed by both UN Groups. It also highlights the rising trends that have been framed as upcoming matters of concern by the 2021 OEWG and the Sixth GGE reports. These concerns still need to be addressed in-depth if the UN aims to stay relevant as a catalyst for normative leadership and governance with the goal to preserve peace and security in cyberspace.

© theblowup, Unsplash

[1] The OEWG final report and the Sixth GGE advanced copy of final report

Comparative Analysis of OEWG and GGE Achievements in 2021

Genesis Behind Two Competitive Processes

Until 2019, the UN Governmental Group of Experts (GGE) was the main authoritative group and formal process mandated to provide the international community with recommendations on how to address the legal, technological, and political challenges posed by cyberspace in the context of international security. Between 2004 and 2016, the United Nations General Assembly (UNGA) established five GGEs, each of which included specialists from 15 to 25 UN member states, including the five permanent members of the Security Council (the P-5). The other delegates for each group were chosen using the UN's formula for equitable geographical distribution.

In 2010, 2013, and 2015, the UN GGE released consensus reports, laying out a fundamental framework for responsible state behaviour and conflict prevention in cyberspace. While non-binding in legal terms, these reports hold substantial normative and political clout, given that they were endorsed by the United Nations General Assembly. The 2010 GGE report contributed to building consensus on the evolving nature of the cyberthreat landscape. For the first time, the 2013 GGE report developed the normative position that international law, including the UN Charter, applies to conflicts and state conduct in cyberspace. Eliciting this normative principle marked the beginning of complex inter-state discussions and tensions about what the applicability of international law in cyberspace implies in practice. The 2015 GGE report comprised a list of eleven non-binding voluntary norms[2] of responsible state behaviour in cyberspace, and, while the report did not explicitly mention international humanitarian law (IHL), it made specific references to its principles of humanity, necessity, proportionality, and distinction.

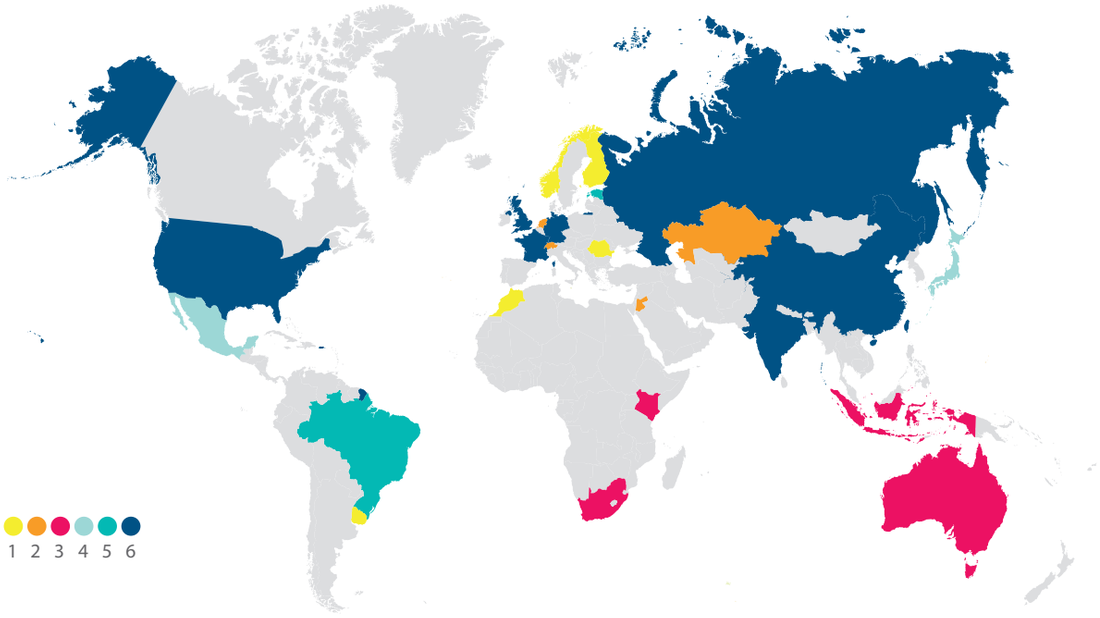
The 2015 GGE norms included critical elements of state conduct in conflict such as restrain to rely on proxies, target infrastructure critical to civilian security and incapacitate emergency-response teams to cyberattacks – commonly called "Computer Emergency Response Team" (CERTS).

In 2017, in a context of state-sponsored cyber operations, including Russia's interference in the 2016 US presidential elections, tensions between powerful tech-leading states resulted in the fifth GGE failing to agree on a report. Failure to reach a consensus came inter alia from diverging perspectives on the applicability of certain principles of international law and IHL to cyberspace, in particular the right of self-defence, state accountability, and countermeasures.

Nonetheless, cyberspace gained significance, not only as a new domain of fierce competition over information, business, and strategic technological operations, but also as a new battlefield for projecting or undermining normative influence. In 2018, Russia sponsored a resolution (73/27) calling for the establishment of a substitute for the GGE – an Open-Ended Working Group (OEWG) – which operates based on consensus, includes all UN member states, and allows participation by interested party from the private sector, academia and civil society organisations. In turn, the United States sponsored a resolution (73/266) calling for the resumption of the GGE – the Sixth GGE on "Advancing Responsible State Behaviour in Cyberspace in the Context of International Security" – which remained consensus-based and comprised of 25 member states. As a majority of states voted in favour of both resolutions, the General Assembly created two parallel and competitive processes with a 90% overlapping mandate (see Figure 1 & 2).

[2] See Annex 1

Figure 1 | Number of GGEs attended by UN member states since 2004



(Source: GPI DigitalWatch & TECH MONITOR)

How are these two UN Cyber Groups influencing each other, particularly given the rise of state-led hostile cyber operations and the context of geopolitical tensions in which these two UN processes were sponsored? The risk is that the multiplication of fora could duplicate and dilute rather than deepen and improve UN efforts as well as international and regional collaborations which already aim to support responsible governance of cyberspace.

The OEWG 2021 Report: A First Step Towards Multilateral and Multistakeholder Positioning on International Cybersecurity?

After nearly two years of deliberations, the adoption by the OEWG of a final report by consensus was an important milestone to forge multilateral positioning on cybersecurity with substantial inputs from multistakeholder groups. Forging agreement on the report was achieved by keeping a short, simplified consensus section for approval and adoption by member states while placing elements still under discussion in the annexed Chair's Summary. The OEWG report sheds light on strategic points of consensus and also makes recommendations for further progress in the areas of emerging threats, voluntary behavioural norms, international law, capacity building, confidence-building measures, and potential formats for regular UN dialogue on international cybersecurity.

- **Endorsing the Acquis of 2010-2015:** The OEWG report reaffirms the acquis, which is the common term used by UN and government officials to refer to the collective outcomes of the UN's GGEs on responsible state behaviour in cyberspace, in particular the three GGEs that agreed on consensus reports in 2010, 2013, and 2015. This fundamental normative framework stipulates, *inter alia*, 1) the applicability of international law to cyberspace, including the UN Charter; and 2) adhesion to 11 non-binding, voluntary norms of responsible state behaviour, with the understanding that further norms could be developed and adopted over time. It is important to note that the OEWG report makes specific reference to the acquis in some of its recommendations, delineating responsible state conduct in cyberspace. For instance, paragraph 31 reminds that, "States should not conduct or knowingly support ICT activity contrary to their obligations under international law that intentionally damages critical infrastructure or otherwise impairs the use and operation of critical infrastructure to provide services to the public," which is one of the 2015 GGE norms. While normative language prohibiting the use of proxies has not been included in the consensus section, the OEWG report, by affirming the acquis, there-

fore endorses the 2013 GGE report's recommendation that "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."

Yet, from attacks on the healthcare sector to interference with electoral and political processes, the current deterioration of security for critical infrastructure, including democratic institutions, is increasingly due to state-led cyber operations that both, rely on proxy actors and target critical civilian infrastructure. This is partially why, during the OEWG proceedings, some governments[3] have called for a legally enforceable instrument, while others, including civil society organizations, have proposed numerous accountability systems and frameworks, none of which have been adopted.

Several civil society organisations have made a compelling case for developing clear and actionable mechanisms to hold states accountable for their conduct in cyberspace. ICT4Peace's proposal for establishing a "Cyber Peer Review" mechanism would have provided for a state-led review process coupled with input from the wider stakeholder community. In its comments on the "Zero Draft" of the OEWG report, the CyberPeace Institute has made an eloquent argument in favour of accountability in cyberspace: "We ask that there be a greater push towards accountability, which requires an inclusive process, evidence-led reporting of attacks, and the advancement of international law. Steps have been taken in this direction, though we re-emphasize the need to keep a human focus on all these issues. We cannot afford to lose this perspective if we are to ensure and protect a secure cyberspace for all." The Institute reiterated that with lack of guidance on accountability and international law applicability in cyberspace, "people will continue to fall victim to cyberattacks and be unsure of their rights, as States are unclear on what actions they can take to hold malicious actors to account."

The reiteration of previous GGE recommendations on voluntary norms and international law, this time in a process which included all UN member states, can still be regarded as one of the main achievements of the OEWG process. It can be seen as a substantive step in reaffirming a set of norms to help countries, including emerging tech-powers, define governance approaches in cyberspace. In the future, such normative frameworks may form the basis to advance collective accountability for hostile cyber operations violating international norms. With the notable exception of Cuba and Iran, a core number of UN member states approved that the OEWG report recognised the collective outcomes of past GGE consensus reports, in particular the content of the UNGA resolution 70/237.[4] In interventions about affirming the acquis, Brazil even hoped that "the adoption of this report by consensus, together with the report of the ongoing GGE, will lead to the return of a unified, universal, collaborative, constructive and consensus-based dialogue process within the United Nations."

- **Divided Positions on IHL and Legally Binding Instruments:** The OEWG proceedings were marked by geopolitical tensions on both, the applicability of IHL to state behaviour in cyberspace and the need for a legally binding instrument or legal framework on international cybersecurity. The final OEWG consensus section did not go beyond the recommendation in paragraph 40 that "States continue to study and undertake discussions within UN future processes as how international law applies to the use of ICTs by States as a key step to clarify and further develop common understanding on this issue." The fact that the consensus report does not mention the exact term "IHL" is one example of a red line that countries in the non-aligned movement (NAM), including China, Cuba and Venezuela, refused to concede. These and other NAM countries argue that accepting a clear reference and further reflection on the applicability of IHL would legitimise conflicts and increased militarisation of cyberspace. The International Committee of the Red Cross (ICRC) argued that the applicability of IHL to conflicts arising in cyberspace should not been interpreted as legitimising cyberwarfare. However,

[3] Including China, Cuba, Venezuela, Egypt, Peru and Ecuador

[4] Resolution adopted by the General Assembly on 23 December 2015 [on the report of the First Committee (A/70/455)] 70/237. Developments in the field of information and telecommunications in the context of international security

the ICRC's intervention did not succeed in preserving a reference to IHL in the final OEWG consensus section.

Many of the countries that oppose IHL applicability, including Russia, Syria, Cuba, Egypt and Iran, with some support from China, consider past GGE findings as shaped by a Western perspective and propose the development of a global legally enforceable instrument or framework. To those states, the inclusion in paragraph 80 of "possible legally binding obligations" is another concession that was made against the interests of the United States, European countries, Israel, and Australia, among others.

At the same time, many nations that have shown normative leadership in developing the acquis through past GGEs would have wished to see the OEWG making more headway in clarifying how and which legal principles of international law are, or should be applied to state behaviour in cyberspace. Several countries, notably the Nordic countries, the Netherlands, Germany, Austria, Slovenia, Argentina, and Chile stressed that a universal framework for cybersecurity in cyberspace should ideally be built on references to the UN Charter, IHL and international human rights law (IHRL). This position was well defended by the Cybersecurity Tech Accord,[5] stating that: "States respectively [should] work to clarify in precise terms how they understand their own obligations under international law – delineating which actions they understand to be permissible and which are not. Not only would such an exchange of views provide transparency and highlight areas of agreement, but it would also promote discussion around areas of disagreement and help reveal gaps in the international legal framework that should be addressed."

- **Transnational Measures for Capacity-Building:** A host of states,[6] including from the global south, showed strong interest in defining principles for capacity-building as a path for more multilateral convergence, alignment, and a strategic way to approach and respond to current cybersecurity divides. A large number of UN member states, including the US, European countries, Cuba, and South Africa, concluded that capacity building is critical to the ability of states to respond to malicious ICT activity, and that they should be guided by a set of principles as presented in paragraph 56, namely: (i) a sustainable, evidence-based, politically neutral and transparent process; (ii) partnerships driven by trust; (iii) respect for human rights, fundamental freedoms, gender sensitivity, inclusivity, and non-discrimination, as well as respect for confidentiality of sensitive information. A voluntary mechanism – in the form of a national survey (paragraph 65) for sharing information on capacity-building efforts – constitutes a concrete and practical recommendation. Non-state participants in the OEWG proceedings, such as the Global Forum on Cyber Expertise Foundation, Kaspersky and the Brandenburg University's Institute for Security and Safety, stressed the importance of multistakeholder engagement for capacity-building in global cybersecurity.
- **Emerging Issues for the International Cybersecurity Agenda:** Discussions during the OEWG proceedings recognised rising issues (paragraph 18) that had not been addressed yet in presence of all UN member states, such as the strategic importance of 1) protecting medical and other critical civilian infrastructure from cyberattacks, 2) securing the public core of the Internet and 3) preventing election interference. The OEWG report also recognizes the importance of capacity building in international law (paragraph 59) and, at China's request, incites governments to report cybersecurity vulnerabilities with diligence (paragraph 28) and to maintain the integrity of the ICT products' supply chain.
- **Regular Institutional Dialogue and Programme of Action (PoA):** Substantial uncertainty remains about optimal and actionable ways forward for a regular UN dialogue on cybersecurity. The final OEWG report did not delineate a clear strategic path for such a dialogue. While a large number of states, including several European countries, Canada and Japan, supported a "Programme of

[5] The Cybersecurity Tech Accord is a public commitment among more than 80 global companies to protect and empower civilians online and to improve cybersecurity by fostering collaboration among global technology companies committed to protecting their customers/users and helping them defend against malicious threats.

[6] Including, South Africa, Costa Rica, the US, Australia, Austria, Estonia, Slovenia, the UK, Japan, Ireland, Canada, New Zealand and the EU

Work", modelled after the 2001 UN Programme of Work on Small Arms and Light Weapons, this proposal was not approved with universal support and is ultimately presented as only one possible option (in paragraph 77). The core features of such a Programme of Action would have consolidated the UN's work on international cybersecurity into a single permanent multilateral process, which would have met regularly around thematic challenges and would have been equipped with UN secretariat support. The final OEWG report mainly asserts in paragraph 74 that "States concluded that any future mechanism for regular institutional dialogue under the auspices of the UN should be an action-oriented process with specific objectives, and building on previous outcomes, and be inclusive, transparent, consensus-driven and results-based." There are risks to see the proposed "cyber Programme of Action" developing as a parallel and competitive process to the second OEWG that will operate from 2021 to 2025 (adopted in December 2020 by UNGA resolution 75/240). Not all UN member states will have the capacity to engage meaningfully in both processes, as South Africa, for instance, who already voiced concerns about duplication of efforts. It remains to be seen how a potential duplication of fora will not only dilute the focus and ownership but will also foster or undermine positive and concrete engagement with multistakeholder groups.

The Sixth GGE 2021 Report: The Challenge of Applying International Law to Cyberspace

The Sixth GGE was mandated to "continue to study, with a view to promoting common understandings and effective implementation, possible cooperative measures to address existing and potential threats in the sphere of information security." While substantive progress is lacking on the adoption and implementation, the 2021 GGE report achieved consensus at a time of extreme tensions: repeated and severe hostile cyber operations targeted UN member states, including GGE members. They not only exhibited sophistication but were also of unprecedented scale, ranging from election interference, cyber espionage to large-scale ransomware attacks (like the one paralyzing SolarWinds).

The 2021 GGE consensus report rests on four critical positions already affirmed in the 2015 report: 1) the applicability of international law to cyberspace, including the UN Charter; 2) adhesion to, and additional understanding of, the 11 voluntary GGE 2015 norms of responsible state behaviour, with the understanding that further norms could be developed and adopted over time; 3) recognition of the need to further develop collective confidence-building, capacity-building and cooperation measures to bridge cybersecurity and governance divides; 4) recognition of the strategic importance for normative efforts towards cyberpeace, which necessitate to engage with international and regional organisations as well as experts from the private sector, academia and civil society organisations.

The one substantial step forward of the final 2021 GGE report is the official acknowledgment that IHL applies to cyber operations during an armed conflict [paragraph 71 (f)]. To solidify this position, the 2021 GGE addressed past arguments made by Russia, China and Cuba during the 2016-2017 GGE proceedings and asserted that the applicability of IHL to a method of warfare does not legitimise warfare: "The Group noted that international humanitarian law applies only in situations of armed conflict. It recalls the established international legal principles, including, where applicable, these principles of humanity, necessity, proportionality and distinction that were noted in the 2015 report. The Group recognised the need for further study on how and when these principles apply to the use of ICTs by States and underscored that recalling these principles by no means legitimises or encourages conflict." This reference constitutes a minimal step forward compared to the consensus section of the OEWG report and aligns with paragraph 12 in the summary of the OEWG Chair, with a mention that "...States underscored that international humanitarian law neither encourages militarisation nor legitimises resort to conflict in any domain."

Yet, the 2021 GGE proceedings confirmed that uncertainty and disagreement remain about *how* IHL applies to cyber hostilities during armed conflict. Important technical questions persist as how to define and qualify, in the context of armed conflict, cyber aggressions or terms of war when they rely exclusively on cyber means. Another salient question is whether datasets can be considered as "object"

with the consequence that adversarial cyber operations targeting civilian data for manipulation or destruction would then violate IHL (see Box 1).

Significant tensions also emerged in discussions about whether international legal rules and principles should have a binding effect in cyberspace. For instance, the 2021 GGE report recognises that there is no multinational consensus on whether sovereignty is a primary rule of international law or merely a principle with no binding effect [paragraph 71 (b)]. The UK firmly insists on sovereignty as a non-binding principle while a growing number of states, including China, France, Germany and several other European countries, are arguing for a binding status.[7] Defining the legal scope of cyber sovereignty has critical implications to distinguish and qualify when remote, offensive cyber operations constitute a sovereignty breach. The 2021 GGE report did not make further progress as whether it is lawful for states to assume collective countermeasures – for instance, by assisting each other in taking countermeasures during conflicts in cyberspace [paragraph 71 (e)]. The 2021 GGE also faced entrenched tensions on the issue of due diligence – the normative notion that states should be aware of and aim to prevent a situation where hostile cyber operations would be operated from their territory [paragraph 71 (g)]. A certain core of UN member states , including France and Germany, consider due diligence as an important rule of international law that could become customary, but this position is not universal and for instance not shared by Israel.

In fine, the 2021 GGE also emphasises the importance of international cooperation and capacity-building with several countries such as Canada, Australia, the Netherlands and Singapore showing leadership in building understanding and capacities related to the field of international law and cyberspace.

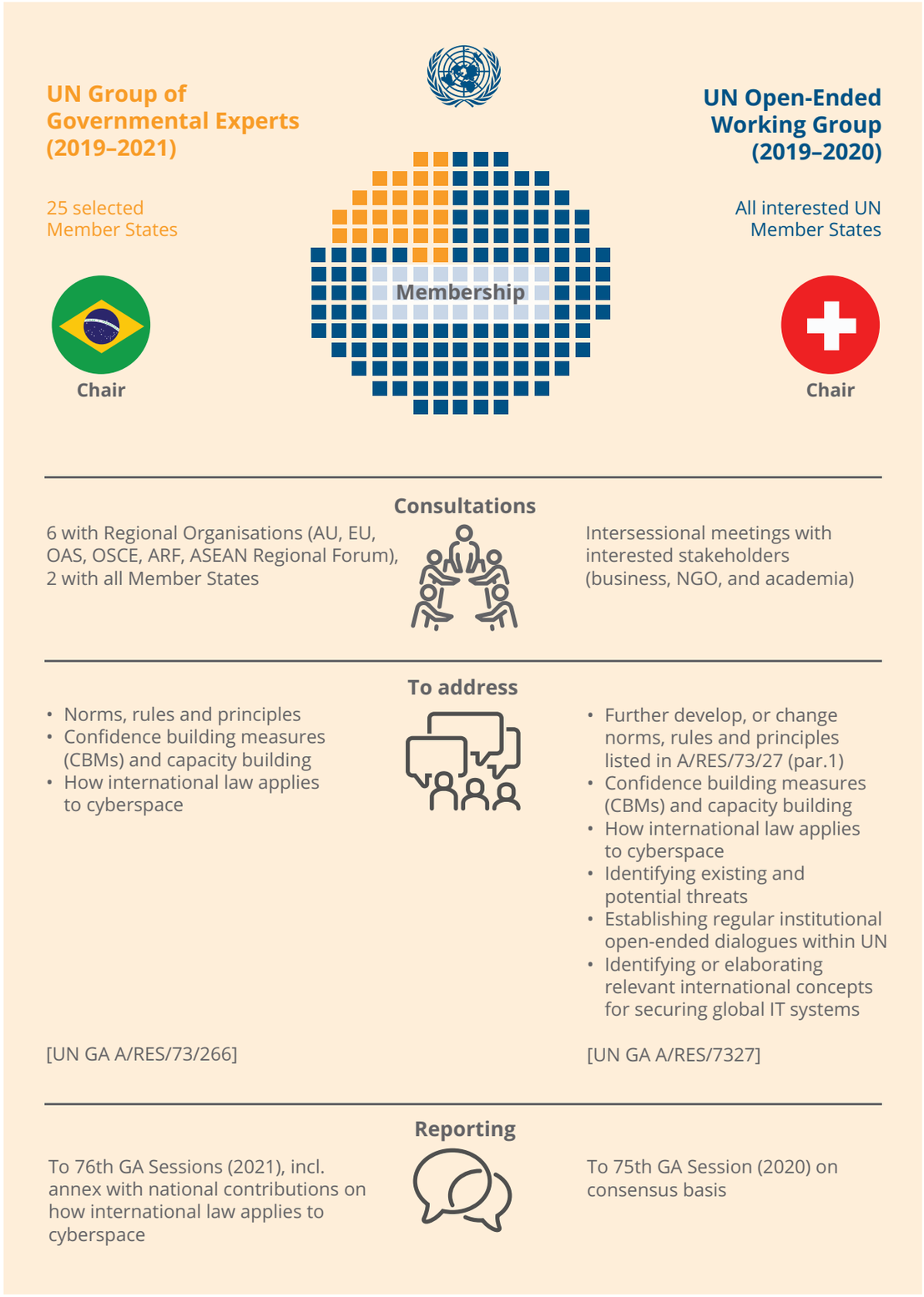
Complementarity and Normative Convergence between UN Cyber Groups

Non-binding in nature, the consensus reports of both UN Cyber Groups reflect normative convergence, in particular around affirming the "acquis" of 2010-2015. Another successful achievement of both Cyber Groups consists in their convening and consultation function, building processes for states and multi-stakeholder actors to exchange arguments and clarify legal positions with increased transparency. Such effort may not only support future political and legal dialogue but also contribute to forming an ***opinio juris***, which could lead to consolidate understanding and implementation of customary international law's rules and principles.

Yet, in the end, both reports present extremely cautious and conservative positions on international law applicability, leaving unresolved most contentious discussions on concrete and legal implementation of international principles and rules that should be guiding responsible state conduct in cyberspace. Similarly, the 11 GGE 2015 norms remain voluntary, their implementation depending on the geostrategic interests and positioning of major cyber powers. In both UN Cyber Groups, preserving a form of normative uncertainty and ambiguity tend to serve powerful tech-leading states, including the P-5, as it gives them leverage to shape international governance and regulation in a way that serves their strategic interests. This leaves limited hopes and conjecture that major cyber powers will be willing to develop in the near future legal mechanisms to effectively regulate cyberspace, even in a context of increasing threats and hostilities.

[7] The positions of France and Germany on what constitutes a sovereignty breach tend to converge. For instance, the French position focuses on the fact that "[a]ny unauthorised penetration by a State of French systems or any production of effects on French territory via a digital vector may constitute, at the least, a breach of sovereignty." Germany's position emphasises that "within its borders, a State has the exclusive right – within the framework of international law – to fully exercise its authority, which includes the protection of cyber activities, persons engaging therein as well as cyber infrastructures in the territory of a State against cyber and non-cyber-related interferences attributable to foreign States." China approaches the concept of sovereignty breach and interference in cyberspace together as follows: "China firmly opposes any country using the Internet to interfere in other countries' internal affairs and believes every country has the right and responsibility to maintain its cyber security and protect the legitimate rights and interests of various parties in cyberspace through national laws and policies." It is interesting to note that China also considers that "countries should respect each other's right to choose their own path of cyber development, model of cyber regulation and Internet public policies, and participate in international cyberspace governance on an equal footing." The role of a cyberdefense force is mentioned: "China will give play to the important role of the military in safeguarding the country's sovereignty, security and development interests in cyberspace."

Figure 2 | Comparison between UN Cyber Groups



(Source: GPI DigitalWatch)

What's Next for Multilateral and Multistakeholder Efforts? Rising International Cyber-Insecurity Trends

Both, the OEWG and the Sixth GGE reports recognise and characterise the evolution of the cyber-threat landscape, highlighting increasing hostile cyber operations that target critical infrastructure (CI), critical information infrastructure (CII) and electoral and political processes. For instance, the OEWG's final report states in paragraph 18 that "Malicious ICT activities against CI and CII that undermine trust and confidence in political and electoral processes, public institutions, or that impact the general availability or integrity of the internet, are also a real and growing concern." In similar words, the 2021 GGE report notes in paragraph 6 that "incidents involving the malicious use of ICTs by states and non-state actors have increased in scope, scale, severity and sophistication" and in paragraph 10 that "harmful ICT activity against critical infrastructure that provides services domestically, regionally or globally… have become increasingly serious." The 2021 GGE report also mentions in paragraph 9 "a worrying increase in States malicious use of ICT-enabled covert information campaigns to influence the processes, systems and overall stability of States." And indeed, in the last five years, disinformation and foreign information operations have impacted the political life and electoral cycle of consolidated, as well as emerging democracies.[8]

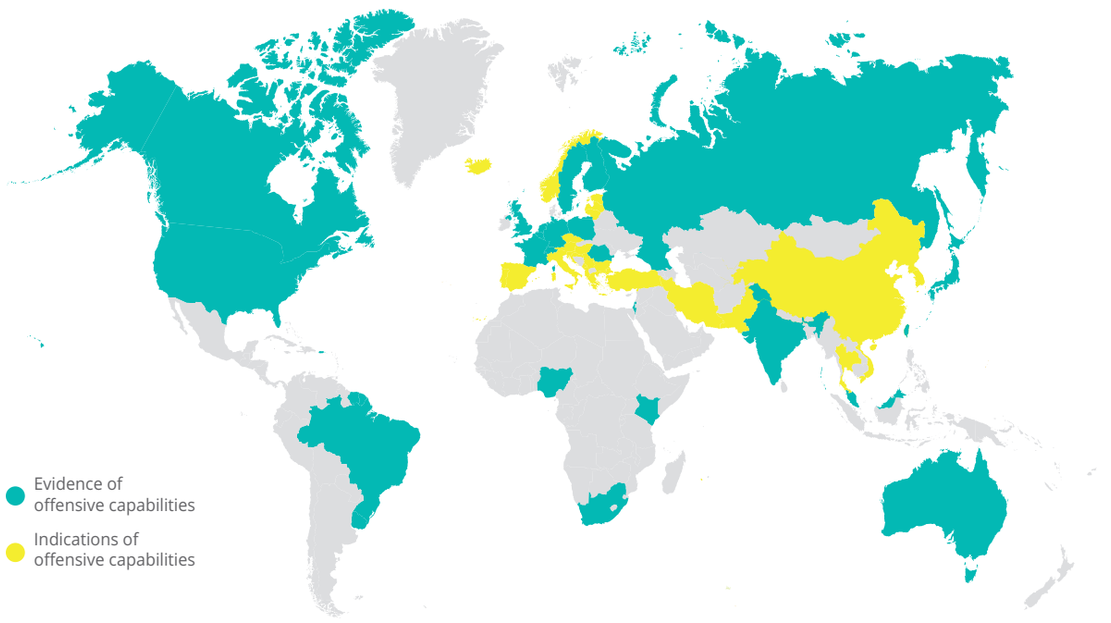
Yet, beyond converging on the "acquis," both UN cyber groups have come short to agreeing on how the voluntary 2015 norms could be translated into a more tangible, accountable and binding normative framework to prevent, mitigate, and respond to the above-mentioned rising cyber-threats.

Since 2015, the cyber-threat landscape has drastically changed. In the wake of the 2015 GGE report, hostile cyber operations targeted the Ukrainian power grid (2015), the 2016 US presidential elections, and inflicted damages of extensive, global proportions with the 2017 WannaCry and NotPetya attacks. During the COVID-19 pandemic, critical medical and biotech infrastructure became rising targets for states and non-state actors alike. The 2021 OEWG consensus report recognises in paragraph 26 that "States further concluded that the COVID-19 pandemic has accentuated the importance of protecting healthcare infrastructure, including medical services and facilities through the implementation of norms addressing critical infrastructure, such as those affirmed by consensus through UN General Assembly resolution 70/237." The 2021 GGE report also mentions in paragraph 10 that "the COVID-19 pandemic has demonstrated the risks and consequences of malicious ICT activities that seek to exploit vulnerabilities in times when our societies are under enormous strain."

The 2021 GGE report reminds us of concerning trends, in particular that states are increasingly investing in offensive cyber capabilities, outlining potential corrosive impact of cyberattacks in both, military and civilian contexts. While (paragraph 7) "the use of ICTs in future conflicts between States is becoming more likely," the GGE report also emphasises that "malicious use of ICT activity by persistent threat actors, including States and other actors, can pose a significant risk to international security and stability, economic and social development, as well as the safety and well-being of individuals" (paragraph 8). Importantly, since 2015 all high-profile cyber operations have fallen short of the definition of an armed attack and hence do not fall under the purview of international humanitarian law. Many of the collective harms caused by states' and non-state actors' misuse of ICT and con-

[8] For further analysis, see: Pauwels, E., The Anatomy of Information Disorders in Africa – Geostrategic Positioning and Multipolar Competition over Converging Technologies, Konrad-Adenauer-Stiftung,, July 2020, ISBN: 978-3-95721-706-6.

Figure 3 | Nations are investing in offensive cyber capabilities, Countries with confirmed or supposed offensive capabilities



(Source: GPI DigitalWatch & TECH MONITOR)

verging technologies take place outside of what could be recognised as an armed conflict.[9] While progress in both UN Cyber Groups has often been stalled over intense debate on IHL applicability, UN processes still need to provide more normative leadership to keep up with the evolving nature of cyber conflict.

Converging Cybersecurity Threats in Grey-Zone Conflicts

UN member states, in particular fragile countries, face a new era of conflicts which are increasingly developing a pervasive cyberspace component. Many landmark studies have documented the recent deterioration of cybersecurity on a global scale and the rising human cost of hostile cyber operations. Cyberattacks worldwide have not only targeted critical civilian sectors, from finance, health to energy, but also industrial control systems, nuclear power plants and complex supply chains, including in biotechnology.[10] Exploiting the pandemics crisis, influence operations have also contaminated social media networks undermining public trust in important elements of civilian security, including scientific and policy emergency measures, as well as governance institutions critical to health, food, political, and economic stability.

The increasing digital reliance of modern societies creates a context of fragility where the convergence of artificial intelligence (AI) with other emerging technologies can augment insecurity. The capacity of computing systems to develop autonomous behaviours will affect life and death scenarios in civilian contexts, outside of traditional military settings. Advances in AI can automate capacity for massive data-optimization, predictive intelligence, systems behavioural analysis, and anomaly detection. Relying on such functional augmentation, AI programs can enable autonomy in other technologies, information infrastructure and industrial platforms (e.g. energy, food, medical, and biotech sectors) that are critical to civilian populations' survival and well-being.

[9] The correct categorization of whether or not an armed conflict exists is important since this will determine whether or not IHL applies. The International Committee of the Red Cross (ICRC), as the guardian of IHL, provides three categories relevant to describe armed conflicts. First, "armed conflict arises whenever there is fighting between States or protracted armed violence between government authorities and organized armed groups or just between organized armed groups." Second, "an international armed conflict arises when one State uses armed force against another State or States." Third, "non-international armed conflicts, also known as internal armed conflicts, take place within the territory of a State and do not involve the armed forces of any other State."

[10] For further analysis, see: USA, Cyberspace Solarium Commission Report, March 2020; Playing with Lives: Cyberattacks on Healthcare are Attacks on People, CyberPeace Institute, March 2021; Advances in Science and Technology to Combat Weapons of Mass Destruction (WMD) Terrorism, UNICRI, June 2021.

What is substantially different in the current age of technological convergence is the potential for AI to enable offensive cyber operations that target and weaponize the interdependence between crucial digital assets and security domains: growing multi-modal and sensitive datasets collected about populations worldwide; data-analytics systems crucial to intelligence and governance (including within multilateral/UN processes); and interconnected, automated industrial platforms and critical infrastructure. Technological convergence therefore deeply impacts how resilient societies will become to new forms of hybrid threats, connecting across security domains, merging civilian and military contexts, and at the boundary between war and peace.

As advances in ICTs, AI and converging technologies amplify potential threats to human security, the nature of conflict is also evolving. Tech-leading nations, cybercriminals and non-state violent actors increasingly engage in "grey zone" conflicts and competitions, perpetrating influence, cyber and information operations as well as covert technological attacks that, while under the threshold of war, may nevertheless cause severe civilian harm. Regional powers like China, the U.S. and, to some extent, Russia, have spent decades acquiring requisite technological and human capital in converging technologies, and have begun competing over digital assets in cyberspace.[11]

In the near-future, **two defining trends** will affect the future of global cybersecurity, and should become part of multilateral and multi-stakeholder normative discussions as well as prevention efforts.

TREND 1: Collective Harms Inflicted on Civilian Critical Infrastructure (CI) and Critical Information Infrastructure (CII)

The 2020-2021 OEWG proceedings allowed important discussions between states, private sector actors and civil society organisations to take place and helped delineate emerging positions on the protection of CI and CII, including health and medical infrastructures.

As mentioned previously, the OEWG report went through several stages of revision before a consensus could be forged. In May 2020, the revised pre-draft of the OEWG report included in the threat section a mention of the vulnerability of CI and CII and made an important note on the transnational character and function of such infrastructures: "CI and CII may be shared or networked with another State or operated across different States and jurisdictions (sometimes categorised as transborder, transnational or supra-national infrastructure)" (paragraph 23). In the same paragraph, the revised pre-draft also specified that ensuring the security of CI and CII may gain from capacity-building through public-private partnerships as well as "inter-State or public-private cooperation may be necessary to protect integrity, functioning and availability." The norm section of the pre-draft insisted on collective responsible efforts towards protection of CI and CII: "States highlighted that the protection of transborder critical information infrastructure, as a distinct category of critical infrastructure, is the shared responsibility of all States" (paragraph 42). The pre-draft connected inter-state cooperation and capacity building as a required approach to protecting transnational CI (paragraph 54).

In March 2021, the final draft of the OEWG report emphasised, as part of the threat analysis, the vulnerability of transnational infrastructure and the subsequent need for inter-state and public-private cooperation: "[critical infrastructure] may be owned, managed or operated by the private sector, may be shared or networked with another State or operated across different States. As a result, inter-State or public-private cooperation may be necessary to protect its integrity, functioning and availability" (paragraph 18). The final OEWG report leaves the definition of CI to the discretion of states but extends the scope by including new examples such as health infrastructure and medical facilities. Australia, the Netherlands, Belgium and the International Committee of the Red Cross (ICRC) welcomed the report's acknowledgement that health infrastructure and medical facilities can be considered CI, while South Africa expressed its agreement with leaving the definition of CI as a national competence.

The progresses made through the 2020-2021 OEWG proceedings are positive but remain limited in light of the growing converging threats to CI and CII. The COVID-19 pandemic provided examples of the growing agility and sophistication of cyberattacks in time

[11] See pp52-62 of the following: Pauwels, E., The Anatomy of Information Disorders in Africa – Geostrategic Positioning and Multipolar Competition over Converging Technologies, Konrad Adenauer Stiftung Foundation, July 2020, ISBN: 978-3-95721-706-6.

of a public health crisis. In December 2020, IBM researchers and the US Cybersecurity and Infrastructure Security Agency (CISA) unveiled global social engineering attacks "intended to steal the network log-in credentials of corporate executives and officials at global organizations involved in the refrigeration process necessary to protect vaccine doses." The underlying goal could have been to access and manipulate shared information about how the vaccine is shipped, stored, kept cold and delivered. Increasingly, states and non-state violent actors can exploit the convergence of AI and emerging cyber-threats to target CI and CII vulnerabilities and amplify risk of adversarial data-manipulation. AI-led cyber-attacks could lead to data-manipulation that generate widespread civilian harms by both, corrupting societies' digital repositories, and compromising the functioning of CI and CII, including industrial control systems. Such rising threats have serious implications for human security, with the potential to manipulate and weaponize safety and governance systems, biomedical and technological infrastructure, critical services and supply chains, as well as scientific and political discourse.

Recent studies[12] in AI- and cybersecurity confirmed that a certain type of deep-learning algorithms can be trained to manipulate the integrity of medical and genomics datasets, expanding a cyber-attack's impact through health, biotech and biosecurity sectors. The adversarial techniques applied to the biotech and medical sectors can transfer to other data-driven domains. Reaching across societies' analytical and data-driven efforts, adversarial information manipulation expands risks to the sabotage of critical infrastructure, industrial platforms, financial, security and governance systems. The capacity of adversarial algorithms to manipulate data-processes and automated protocols provides an increasing potential to weaponize cities' smart civilian technologies, cloud-based industrial platforms, safety control systems and manufacturing supply chains. In 2018, a petrochemical company with a plant in Saudi Arabia was targeted by a new kind of cyberattack, not designed to shut down operations, but to compromise its safety protocols and trigger an explosion.

Due to the interconnectedness of cyberspace, adversarial manipulation of automated and industrial safety protocols could lead to the subsequent shut-down of primary critical systems, from medical equipment, emergency communications, electric grid, levees and dams, to drinking water distribution and sewage management. Early warnings might not be detectable. The harm could be done remotely, on a large scale, and spill-over to essential humanitarian/civilian services provided to populations.

Rising threats to population datasets and civilian infrastructure would also seriously undermine citizens' trust – trust in the accuracy of emergency data-systems, clinical-trials, medical counter-measures (such as vaccines and other therapeutic agents), and data-based research efforts. In turn, malicious actors – states and non-state actors alike – may seize this moment of public distrust for criminal gains, competitive advantage in value and supply chains as well as for commercial and geostrategic influence.

NEXT STEPS ON TREND 1 WITHIN MULTILATERAL FORUMS: The evolving cyber-threat landscape confronts member states and multilateral institutions with increasingly complex questions that will need to be addressed in future UN Cyber Groups. One of them is how to define and characterise in legal terms "adversarial data-manipulation," that may be considered below the threshold of war, but could still produce extensive civilian harm and contaminate an array of critical, essential interconnected services? In the future, the development and implementation of accountability and remedy mechanisms should be discussed and should include the collective data-harms that could be inflicted on civilian populations. In this context, where datasets and data-processes might become a more strategic target than physical objects, member states should be encouraged to further cooperate and build capacity to identify and protect national and transnational CI and CII.

TREND 2: Electoral Interference

In a geopolitical context of rising disinformation campaigns and cyber operations designed to undermine elections, civil society organisations and governments from liberal democratic states have framed the protection of electoral infrastructure and electoral processes as a rising issue to be discussed

[12] Mirsky, Yisroel, et al. CT-GAN: Malicious Tampering of 3D Medical Imagery Using Deep Learning. Arxiv.org, January 2019; Finlayson, Samuel G., et al. « Adversarial Attacks on Medical Machine Learning ». Science (New York, N.Y.), vol. 363, no 6433, mars 2019, p. 1287 89; Allyn, Jérôme, et al. « Adversarial attack on deep learning-based dermatoscopic image recognition systems ». Medicine, vol. 99, no 50, December 2020.

Box 1 | Is data considered an "object" for the purposes of IHL?[13]

The below table and analysis (source) by Taťána Jančárková[14] & Kubo Mačák[15] unveil the legal ambiguity related to computer data as "object" and could be a starting point for further analysis of the qualification of adversarial data-manipulation in the IHL doctrine as it applies to cyberspace:

"The definition of military objectives and the prohibition of attacks on civilian objects are limited to 'objects.' If the target of a cyber operation is not an 'object,' then actions against it are not constrained by the rules of IHL that govern targeting. It is therefore of crucial importance whether data may qualify as an 'object' and therefore be either a military objective subject to attack or a civilian object protected from attack, particularly with respect to cyber operations that do not result in a physical effect. If data does not qualify as an 'object,' civilian datasets would enjoy little, if any, protection in times of armed conflict."

Scenarios	Data considered as object	Data not considered as object
Incident 1 (cyberoperations against military datasets)	Permissible insofar as the dataset fulfils both prongs of the definition of military objectives	Because data is not an "object" for the purposes of IHL, it does not need to fulfil the criteria of a military objective for an operation against it to be lawful under IHL. Accordingly, provided that other applicable rules of IHL are complied with, all of these cyberoperations would be permissible under IHL.
Incident 2 (cyberoperations against essential civilian datasets)	Prohibited due to the non-military character and use of the datasets in question	
Incident 3 (cyberoperations against non-essential civilian datasets)	Prohibited due to the non-military character and use of the datasets in question unless justified under the customary exception for psychological operations and propaganda	

within both UN Cyber Groups. During the OEWG proceedings, election interference has been framed as a threat by several states: New Zealand made reference to "targeted efforts to undermine political systems and elections;" Switzerland mentioned information operations "to undermine trust and confidence in political and democratic processes and institutions;" and Ecuador connected threats to election infrastructure with proposals concerning national infrastructure protection. In 2019, early in the OEWG proceedings, Australia made an interesting argument about addressing election interference under the international law section stating that "the use by a hostile State of cyber operations to manipulate the electoral system to alter the results of an election in another State, intervention in the fundamental operation of Parliament, or in the stability of States' financial systems would constitute a violation of the principle of non-intervention." The well-accepted prohibition on intervention in another state's affairs was mentioned in the 2013 and 2015 GGE reports. The 2021 GGE report brings a subtle layer of understanding by noting that intervention can be both, direct or indirect. For instance, a state could rely on cyber operations to directly interfere with the conduct of an election in another state, or could use adversarial information operations to create enough public distrust and social unrest to severely destabilise government authorities.

[13] For further analysis, see: Kubo Mačák, 'Military Objectives 2.0: The Case for Interpreting Computer Data as Objects under International Humanitarian Law' (2015) 48 IsrLR 55, 77–80.

[14] Ms. Taťána Jančárková, NATO Co-operative Cyber Defence Centre of Excellence

[15] Dr. Kubo Mačák, International Committee of the Red Cross

Further down the line, as OEWG discussions progressed, several states' positions solidified around the importance of relying on measures or norms to protect the integrity of electoral infrastructure and processes. Brazil specified that "the IT infrastructure underpinning electoral processes also deserve the same protection accorded to the public core of the Internet." The Netherlands and Germany were both in favour of normative leadership on this issue: the two countries proposed a norm that aims to protect the "technical infrastructure essential to political processes, such as elections, referenda or plebiscites" and framed this norm as a potential guidance for implementation of UN GGE 2015 norms on critical infrastructure protection. The final OEWG report retained some of the above states' emphasis on framing as a "threat," the vulnerability of the infrastructure underlying political and electoral processes.

On this rising trend of electoral interference, it is important to note a relative convergence between different UN member states. In their position papers submitted in the context of the Sixth GGE proceedings, France, Israel and Germany progressively converged with Australia's argument that electoral interference could constitute a violation of the principle of non-intervention. Germany's framing of the issue is particularly clear:

"In the context of wrongful intervention, the problem of foreign electoral interference by means of malicious cyber activities has become particularly virulent. Germany generally agrees with the opinion that malicious cyber activities targeting foreign elections may – either individually or as part of a wider campaign involving cyber and non-cyber-related tactics – constitute a wrongful intervention. For example, it is conceivable that a State, by spreading disinformation via the internet, may deliberately incite violent political upheaval, riots and/or civil strife in a foreign country, thereby significantly impeding the orderly conduct of an election and the casting of ballots. […] Also, the disabling of election infrastructure and technology such as electronic ballots, etc. by malicious cyber activities may constitute a prohibited intervention, in particular if this compromises or even prevents the holding of an election, or if the results of an election are thereby substantially modified."

States will learn to live with emerging types of electoral cyber-threats, just as they are learning to apprehend the shifting nature and scope of low-intensity cyber conflict. A rising concern is that with AI and increasing cyber interconnectedness; these threats to election security will become more complex, difficult to prevent and detect.[16] They will target national information infrastructure, undermining the integrity of sensitive security and civilian biometrics data. Elections – like other data-driven infrastructures in health – are vulnerable to emerging techniques of data-manipulation. And, like trust in health services, trust in elections is at the core of our social contract, the foundation of our democracies.

In the last five years, hacks of electoral and biometrics datasets have exposed the dangers of extensive breaches of sensitive information, from ethnic backgrounds, personal profiles to online behaviours. Large-scale voters' data exfiltration has already impacted populations in the US, Israel, India, Kenya and the Philippines, to name but a few. With this recent deterioration of cybersecurity, populations' datasets and their related electoral infrastructure are growing target for data-manipulation. For the multilateral system, it is therefore urgent to anticipate and mitigate how the convergence of AI, cyber-threats and data-capture technologies can be misused to discredit electoral institutions, influence populations' behaviours, and erode citizens' trust and political agency. In fragile and conflict-prone countries, undermining trust in elections often threatens internal peace and civilian security.

NEXT STEPS ON TREND 2 WITHIN MULTILATERAL FORUMS: Considering the peace and security implications, protecting electoral institutions from technological and data-harms is becoming a multilateral obligation. There is a growing number of states that have taken position on the applicability of international law in cyberspace with some of them willing to consider election interference as a possible violation of the principle of non-intervention. The issue of election interference might become increasingly relevant to how states define the scope of cyber sovereignty.

Prevention, mitigation and responses to election interference could be integrated into inter-state and multi-stakeholder cooperation on capacity-building. It could be supported within a regular institutional mechanism such as the Programme of Action, proposed in paragraph 77 of the final OEWG report. In the context of a PoA, the UN and its member states could bolster agile multi-stakeholder engagement where electoral management bodies, civil society and private sector actors could better forecast fast-emerg-

ing threats as well as develop and operationalize conflict-sensitive, electoral safeguards and robust accountability frameworks. For instance, as recommended by civil society organisations such as the CyberPeace Institute, multi-stakeholder partnerships could promote a culture of responsible governance that relies on a human-centred understanding of risks and vulnerabilities in ICTs and election technology, looking at the entire election cyber ecosystem with human behaviour as an integral part of it.

CONCLUSION

The success of both UN Cyber Groups is of diplomatic and strategic nature. The most important achievements of the OEWG and the Sixth GGE is the engagement and knowledge-sharing between UN member states and major non-state players, including regional organisations, private sector, academia and civil society. Several delegations mentioned that the OEWG has contributed to build understanding among all member states on complex, timely and transnational challenges faced in cyberspace. For instance, the representative of Malaysia noted that "My delegation has benefited tremendously from the opportunity to better understand various issues on ICTs and the underlying nuances, by listening directly to the clear articulations of positions and arguments by distinguished delegates." Such exchange of arguments and positions is not only the basis for further political and legal dialogue that may forge normative consensus, but also the basis for a form of "opinion juris" that may have a substantial impact on the future development of customary international law. The collective efforts demonstrated by an array of states and non-state actors through proceedings and consultations at the OEWG and the Sixth GGE may have further implications. These efforts may be a first step to subsequently develop alliances, expertise and confidence so that future capacity-building efforts could benefit states that are not leading cyber powers, yet, are already targets of hostile cyberattacks and information operations.

Beyond these incremental diplomatic successes, the two UN Cyber Groups did not achieve fundamental progress that would reflect the ability and the will of the major cyber powers to effectively regulate cyberspace. The lack of trust between tech-leading nations and the pursuit of their geostrategic interests reinforce the diagnosis that the two consensus-based UN groups are not necessarily the best mechanism to exert normative leadership in a context of converging cybersecurity threats. Six years after the adoption of the "acquis," the two UN groups still fall short of translating the 2015 voluntary norms of responsible behaviour into a clear, reasonable and enforceable normative framework. Both forums also fail to acknowledge the important role that accountability processes could play to hold states accountable for their conduct in cyberspace.

The cybersecurity threats landscape will keep evolving and, under the impulse of technological convergence, may drastically change in the next decade. UN member states and the multilateral system are not prepared or equipped to regulate and mitigate the cyber- and information security challenges triggered by the convergence of AI, automation and cybersecurity. As explained in section 2, a substantive amount of technical, normative and legal analysis is needed to understand how the doctrine, rules and principles of international law can be applied to situations where offensive cyber operations do not trigger the threshold of conflict but target digital, intangible and non-physical civilian assets (CI and CII). Similarly, emerging tech-enabled phenomena – such as AI and cyber election interference – could become relevant to international law, *inter alia* the principle of non-intervention. However, such a complex argument does not yet have universal support. An alliance of like-minded states would be well-advised to engage in a concerted process for mapping all current and potential divergences in international legal frameworks applicable to cyberspace and cybersecurity, properly analyse these divergences, and find consensus on whether, and how, to settle each one. Such effort would gain from relying on regular institutional dialogue and continuous forms of multistakeholder engagement and knowledge-sharing. Such an initiative could then inform and feed into the multilateral fora which are needed in order to forge an international consensus. The near-future will tell us if the 2021-2025 OEWG or another mechanism – such as the Program of Action – can support normative foresight and leadership on international cybersecurity.

[16] For further analysis, see: Pauwels, E., Cyber-AI Convergence and Interference – Securing Elections and Building Human Resilience, Konrad Adenauer Stiftung Foundation, November 2020.

Bibliography

UN Cyber Groups Documents

UN GA. 2021. Resolution Adopted by the General Assembly on 31 December 2020 on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security. A/Res/75/240, 4 January.

UNGA. 2018. 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.

UNGA. 2018. Resolution Adopted by the General Assembly on 5 December 2018 on Developments in the Field of Information and Telecommunications in the Context of International Security. A/RES/73/27.

UNGA. 2015. Resolution Adopted by the General Assembly on 23 December 2015 on Developments in the Field of Information and Telecommunications in the Context of International Security. A/RES/70/237.

UN GGE

UN GGE. 2021. (Advanced Copy, 28 May 2021). Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. https://front.un-arm.org/wp-content/uploads/2021/06/final-report-2019-2021-gge-1-advance-copy.pdf

UN GGE. 2010. Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. UNGA. A/65/201 New York: UN.

UN GGE. 2013. Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. UN Doc A/68/98, 24 June. https://undocs.org/A/68/98.

UNGGE. 2015. Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. UN Doc A/70/174, 22 July. https://undocs.org/A/70/174.

OEWG

Chair of the OEWG. 2020. Initial 'Pre-draft' of the report of the OEWG on developments in the field of information and telecommunications in the context of international security. 27 April. https://unoda-web.s3.amazonaws.com/wp-content/uploads/2020/03/200311-Pre-Draft-OEWG-ICT.pdf

Chair of the OEWG. 2020. Second 'Pre-draft' of the report of the OEWG on developments in the field of information and telecommunications in the context of international security. 27 May. https://front.un-arm.org/wp-content/uploads/2020/05/200527-oewg-ict-revised-pre-draft.pdf

Chair of the OEWG. 2021a. Draft Substantive Report (Zero Draft) of the report of the OEWG on developments in the field of information and telecommunications in the context of international security. 19 January. https://undocs.org/A/AC.290/2021/L.2.

Chair of the OEWG. 2021b. Substantive Report (First Draft) of the report of the OEWG on developments in the field of information and telecommunications in the context of international security. 1 March. https://front.un-arm.org/wp-content/uploads/2021/03/210301-First-Draft.pdf

Chair of the OEWG. 2021. Final Substantive Report of the report of the OEWG on developments in the field of information and telecommunications in the context of international security. 10 March. https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf

Chair of the OEWG. 2021. Chair's Summary of the OEWG on developments in the field of information and telecommunications in the context of international security. 10 March. https://front.un-arm.org/wp-content/uploads/2021/03/Chairs-Summary-A-AC.290-2021-CRP.3-technicalreissue.pdf

Compendium of statements in explanation of position on the final report, Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security Third substantive session, 8–12 March 2021. A/AC.290/2021/INF/2. https://front.un-arm.org/wp-content/uploads/2021/04/A-AC.290-2021-INF-2.pdf

Australia. 2019. Australian paper – Open Ended Working Group on developments in the field of information and telecommunications in the context of international security, September 2020. https://unoda-web.s3.amazonaws.com/wp-content/uploads/2019/09/fin-australian-oewgnational-paper-Sept-2019.pdf.

Brazil. 2020. Comments submitted by Brazil to the Initial 'Pre-draft' of the report of the OEWG on developments in the field of information and telecommunications in the context of international security.https://front.un-arm.org/wp-content/uploads/2020/04/comments-by-brazil-on-the-predraft-report-of-cyber-oewg-8-apr-2020.pdf

Ecuador. 2020. Ecuador preliminary comments to the Chair's 'Initial pre-draft' of the Report of the United Nations Open Ended Working Group on developments in the field of information and telecommunications in the context of international security (OEWG). https://front.un-arm.org/wpcontent/uploads/2020/04/ecuador-comments-on-initial-pre-draft-oewg.pdf

France. 2020. France's response to the pre-draft report from the OEWG Chair. https://front.un-arm.org/wp-content/uploads/2020/04/contribution-fr-oewg-eng-vf.pdf

Germany. 2020. Initial 'Pre-draft' of the report of the OEWG on developments in the field of information and telecommunications in the context of international security and non-paper listing specific language proposals under agenda item 'Rules, norms and principles' from written submissions received before 2 March 2020. Comments from Germany. https://front.un-arm.org/wp content/uploads/2020/04/20200401-oewg-german-written-contribution-to-pre-draft-report-1.pdf

Germany. 2021. Position Paper by the Federal Government on the Application of International Law in Cyberspace. https://www.auswaertiges-amt.de/blob/2446304/32e7b2498e10b74fb17204c54665bdf0/on-the-application-of-international-law-in-cyberspace-data.pdf

New Zealand. 2020. Position Paper on New Zealand's Participation in the February 2020 Session of the 2019-2020 Open Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security. https://unoda-web.s3.amazonaws.com/wp-content/uploads/2020/02/nz-position-paper-on-oewg.pdf

South Africa. 2020. Comments on the "Pre-draft" of the report of the UN Open Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security. https://front.un-arm.org/wp-content/uploads/2020/04/south-africa-inputs-of-oewg-predraft.pdf

South Africa. 2021. Statement by South Africa at the Informal Meeting of the UN Open Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security, 22 February 2021. https://front.un-arm.org/wp-content/uploads/2021/02/South-Africa-statement-OEWG-Final.pdf

Switzerland. 2020. UN Open-ended working group on developments in the field of information and telecommunications in the context of international security, 2019/2020 Written feedback by Switzerland to the first pre-draft report of the OEWG. https://front.un-arm.org/wp-content/uploads/2020/04/20200409-switzerland-remarks-oewg-pre-draft.pdf

The Netherlands. 2020c. The Kingdom of the Netherlands' response to the pre-draft report of the OEWG. https://front.un-arm.org/wp-content/uploads/2020/04/kingdom-of-the-netherlandsresponse-pre-draft-oewg.pdf

Comments by the CyberPeace Institute on the "Zero Draft" of the report of the OEWG on developments in the field of information and telecommunications in the context of international security. https://front.un-arm.org/wp-content/uploads/2021/02/CyberPeace-Institute-UNOEWGZeroDraftComments_CyberPeaceInstitute.pdf

Comments by ICT4Peace Foundation on the "Zero Draft" of the report of the OEWG on developments in the field of information and telecommunications in the context of international security. https://front.un-arm.org/wp-content/uploads/2021/02/cyber-ict4p-comment-zero-draft-feb-2021.pdf

Comments by the International Committee of the Red Cross (ICRC) on the Substantive Report [First Draft] of the 'Open-ended working group on developments in the field of information and telecommunications in the context of international security. https://front.un-arm.org/wp-content/uploads/2021/03/ICRC-Comments-on-the-First-Draft-of-the-OEWG-Report.pdf

Comments by the Cybersecurity Tech Accord on the Substantive Report [First Draft] of the 'Open-ended working group on developments in the field of information and telecommunications in the context of international security. https://front.un-arm.org/wp-content/uploads/2021/03/Tech-Accord-OEWG-response-March-2021-FINAL.pdf

Comments by the Global Forum on Cyber Expertise ("GFCE") Foundation on the Substantive Report [First Draft] of the 'Open-ended working group on developments in the field of information and telecommunications in the context of international security. https://front.un-arm.org/wp-content/uploads/2021/03/GFCE-Comments-on-OEWG-First-Draft.pdf

Comments by the Institute for Security and Safety GmbH (ISS), Brandenburg University of Applied Sciences, on the Substantive Report [First Draft] of the 'Open-ended working group on developments in the field of information and telecommunications in the context of international security. https://front.un-arm.org/wp-content/uploads/2021/02/Institute-for-Security-and-Safety-ISS-OEWG-Zero-Draft-comments_220221.pdf

Comments by Kaspersky ("Kaspersky Position Paper") on the Substantive Report [First Draft] of the 'Open-ended working group on developments in the field of information and telecommunications in the context of international security. https://front.un-arm.org/wp-content/uploads/2021/02/kaspersky-submission-to-the-un-oewg-zero-draft.pdf

Other References

Allyn, Jérôme et al. 'Adversarial attack on deep learning-based dermatoscopic image recognition systems'. Medicine, vol. 99, no 50 (December 2020).

CyberPeace Institute, Playing with Lives: Cyberattacks on Healthcare are Attacks on People, March 2021.

Finlayson, Samuel G. et al. 'Adversarial Attacks on Medical Machine Learning'. Science, vol. 363, no 6433 (March 2019).

ICRC Expert Meeting 14-16 November 2018, "The Potential Human Cost of Cyber Operations". Report prepared and edited by Laurent Gisel, senior legal adviser, and Lukasz Olejnik, scientific adviser on cyber, International Committee of the Red Cross, June 2019.

Mačák K., 'Military Objectives 2.0: The Case for Interpreting Computer Data as Objects under International Humanitarian Law' (2015) 48 IsrLR 55, 77–80.

Mirsky, Yisroel et al. 'CT-GAN: Malicious Tampering of 3D Medical Imagery Using Deep Learning', Cornell University, January 2019.

Pauwels, Eleonore. 'The New Geopolitics of Converging Risks', United Nations University 2019.

Pauwels, E., Cyber-AI Convergence and Interference – Securing Elections and Building Human Resilience, Konrad Adenauer Stiftung Foundation, November 2020.

Pauwels E., Peacekeeping in an Era of Converging Technologies and Security Threats, Research Paper published in the context of the Strategy for the Digital Transformation of UN Peacekeeping, UN Department of Peacekeeping Operations, April/August 2021.

Pauwels E., Cyber-Biosecurity: How to protect biotechnology from adversarial attacks, Hybrid CoE Strategic Analysis / 26, May 2021.

Sanger, David E. & LaFraniere, Sharon. 'Cyberattacks Discovered on Vaccine Distribution Operations', The New York Times, 3 December 2020.

Sanger D., Barnes E. J., and Perlroth N., Preparing for Retaliation Against Russia, U.S. Confronts Hacking by China, New York Times, March 21, 2021.

Väljataga A., Tracing opinio juris in National Cyber Security Strategy Documents, NATO Cooperative Cyber Defence Centre of Excellence, 2018.

TrendMicro Research/Europol's European Cybercrime Centre/UNICRI , 2020 Report - Exploiting AI: How Cybercriminals Misuse and Abuse AI and ML, November 2020.

UNICRI, "Covid-19, Crime Prevention and Criminal Justice Priorities: A Spotlight on Vulnerable Groups," Summary Report, December 2020.

UNICRI, Advances in Science and Technology to Combat Weapons of Mass Destruction (WMD) Terrorism, report developed by UNICRI's Knowledge Center Security through Research, Technology and Innovation (SIRIO), June 2021.

United States of America's Cyberspace Solarium Commission Report, Co-Chairmen Senator Angus King (I-Maine) and Representative Mike Gallagher (R-Wisconsin), published March 2020.

Author:
Eleonore Pauwels

Eleonore Pauwels is an international expert in the security, societal and governance implications generated by the convergence of artificial intelligence with other dual-use technologies, including cybersecurity, genomics and genome-editing. Pauwels provides expertise to the World Bank, the United Nations and the Global Center on Cooperative Security in New York. She also works closely with governments and private sector actors on AI-Cyber Prevention, the changing nature of conflict, foresight and global security. In 2018 and 2019, Pauwels served as Research Fellow on Emerging Cybertechnologies for the United Nations University's Centre for Policy Research. At the Woodrow Wilson International Center for Scholars, she spent ten years within the Science and Technology Innovation Program, leading the Anticipatory Intelligence Lab. She is also part of the Scientific Committee of the International Association for Responsible Research and Innovation in Genome-Editing (ARRIGE).

Pauwels is a former official of the European Commission's Directorate on Science, Economy and Society. Pauwels regularly testifies before U.S. and European authorities including the U.S. Department of State, NAS, NIH, NCI, FDA, the National Intelligence Council, the European Commission and the UN. She writes for Nature, The New York Times, The Guardian, Scientific American, Le Monde, Slate, UN News, The UN Chronicle and The World Economic Forum

Annex 1

UNGGE. 2015. Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. UN Doc A/70/174, 22 July. https://undocs.org/A/70/174. Excerpt, from paragraph 13, p 7-8:

13. Taking into account existing and emerging threats, risks and vulnerabilities, and building upon the assessments and recommendations contained in the 2010 and 2013 reports of the previous Groups, the present Group offers the following recommendations for consideration by States for voluntary, non-binding norms, rules or principles of responsible behaviour of States aimed at promoting an open, secure, stable, accessible and peaceful ICT environment:

(a) Consistent with the purposes of the United Nations, including to maintain international peace and security, States should cooperate in developing and applying measures to increase stability and security in the use of ICTs and to prevent ICT practices that are acknowledged to be harmful or that may pose threats to international peace and security;

(b) In case of ICT incidents, States should consider all relevant information, including the larger context of the event, the challenges of attribution in the ICT environment and the nature and extent of the consequences;

(c) States should not knowingly allow their territory to be used for internationally wrongful acts using ICTs;

(d) States should consider how best to cooperate to exchange information, assist each other, prosecute terrorist and criminal use of ICTs and implement other cooperative measures to address such threats. States may need to consider whether new measures need to be developed in this respect;

(e) States, in ensuring the secure use of ICTs, should respect Human Rights Council resolutions 20/8 and 26/13 on the promotion, protection and enjoyment of human rights on the Internet, as well as General Assembly resolutions 68/167 and 69/166 on the right to privacy in the digital age, to guarantee full respect for human rights, including the right to freedom of expression;

(f) A State should not conduct or knowingly support ICT activity contrary to its obligations under international law that intentionally damages critical infrastructure or otherwise impairs the use and operation of critical infrastructure to provide services to the public;

(g) States should take appropriate measures to protect their critical infrastructure from ICT threats, taking into account General Assembly resolution 58/199 on the creation of a global culture of cybersecurity and the protection of critical information infrastructures, and other relevant resolutions;

(h) States should respond to appropriate requests for assistance by another State whose critical infrastructure is subject to malicious ICT acts. States should also respond to appropriate requests to mitigate malicious ICT activity aimed at the critical infrastructure of another State emanating from their territory, taking into account due regard for sovereignty;

(i) States should take reasonable steps to ensure the integrity of the supply chain so that end users can have confidence in the security of ICT products. States should seek to prevent the proliferation of malicious ICT tools and techniques and the use of harmful hidden functions;

(j) States should encourage responsible reporting of ICT vulnerabilities and share associated information on available remedies to such vulnerabilities to limit and possibly eliminate potential threats to ICTs and ICT-dependent infrastructure;

(k) States should not conduct or knowingly support activity to harm the information systems of the authorized emergency response teams (sometimes known as computer emergency response teams or cybersecurity incident response teams) of another State. A State should not use authorized emergency response teams to engage in malicious international activity.

Konrad-Adenauer-Stiftung e. V.

Andrea E. Ostheimer
Executive Director
www.kas.de/newyork

andrea.ostheimer@kas.de

ISBN: 978-1-7369528-2-5