THE UNITED NATIONS' CONTRIBUTIONS TO ENHANCE GLOBAL CYBERSECURITY: AN ASSESSMENT OF ITS REGULATORY BODIES' SUCCESSES AND CHALLENGES

LARA MARIA GUEDES GONÇALVES COSTA

ABSTRACT

The United Nations (UN) has played a key role in inter-state discussions on cybersecurity in the past years. The UN Group of Governmental Experts (GGE) and the Open-ended Working Group (OEWG) are among the most prominent international regulatory bodies addressing the challenges of emerging and disruptive technologies, calling for state cooperation and a common approach to these issues. This article explores the progress of the GGE and OEWG from their creation to the present and analyses the enduring sources of contention between states in cybersecurity affairs. In particular, it discusses the challenges of applying international law and international humanitarian law to cybersecurity and developing global legal norms. It also analyses the GGE and OEWG reports to evaluate their achievements, shedding light on ongoing cybersecurity efforts and issues at the international level.

Keywords: *United Nations; GGE; OEWG; cybersecurity; international law; international humanitarian law; UN Charter.*

INTRODUCTION

Cybersecurity, defined as the ethical, legal, and safe use of cyberspace by states, has become one of the key priorities of the United Nations (UN). In light of growing concerns over the misuse of information and communications technologies (ICTs), the UN Common Agenda's report addresses major cybersecurity challenges, including cyber attacks and cyber warfare, calling upon states to cooperate for peace and security (United Nations, 2021c). Cyberspace has become a contested environment where countries conduct offensive cyber operations against other states, violating information protection and targeting critical infrastructures (CSIS, 2022). The cyber attacks suffered by Estonia and Georgia in the early 2000s, and more recently by Ukraine (2014-present), have increased awareness of cybersecurity and the prominence of cyber-related issues (Tiirmaa-Klaar, 2021: 4; Willett, 2022; Levite, 2023). At the same time, different countries' approaches to cybersecurity have highlighted their diverging perspectives and interests, which have been difficult to reconcile.

Amidst such complex divergences, UN efforts have been essential to enhancing cybersecurity. Within the UN system, the Group of Governmental Experts (GGE) and the Open-ended Working Group (OEWG) play a crucial role in supporting the attempts of the UN to adapt to a changing security environment, bringing together UN member states to discuss norms, regulations, and state behaviour in cyberspace (Digital Watch, 2023). The crux of these GGE and OEWG discussions consists in addressing whether and how international law – particularly the UN Charter – and International Humanitarian Law (IHL) should be applied to the digital environment. Regarding this, countries debate the need for new international norms that could fill potential gaps in current international frameworks (Glen, 2021: 1128-1131). Although IHL is a branch of international law, for the purpose of this article's analysis, the terms will be used with different and specific meanings – as in the GGE and OEWG discussions. Hence, international law is understood as the body of agreements between countries – treaties or conventions, such as the UN Charter –, customary rules considered as legally binding, and general principles. IHL is defined as the set of rules and principles (such as distinction and attribution) which seek, for humanitarian purposes, to limit the effects of armed conflict and protect the affected populations (United Nations, 2022; ICRC, 2022b).

Over the years, the GGE and OEWG have released several reports informing the international community on states' progress in finding common ground in cyber affairs (Digital Watch, 2023). The reading of such reports enables reflections on the challenges posed by countries' diverging interests and views, as well as contrasting interpretations of norms and principles. Although the UN's activities around cybersecurity are fragmented throughout the UN system (Henderson, 2021: 583), the GGE and the OEWG are considered prominent initiatives addressing global cybersecurity. Hence, it is worth analysing their work to shed light on inter-state relations in cyberspace.

This article posits that despite UN efforts to enhance international cooperation and regulate state behaviour in cyberspace in a manner consistent with principles of international law, key participating states have been reluctant to collaborate in achieving concrete and binding results in order to preserve their sovereign control over their national cyber-ecosystem and keep open their options of deploying their own cyber-capabilities according to their national interests in the global arena. To substantiate this assertion, it analyses the role of the UN in facilitating state-level cybersecurity discussions by answering the following questions: 1) How have the GGE and OEWG supported the UN system in responding to global cybersecurity issues?; 2) What cybersecurity challenges do the GGE and OEWG still need to address? and 3) What factors constrained the work of the GGE and OEWG on cybersecurity? To answer these questions, the article first explores the roles of the GGE and OEWG in supporting the UN system's responses to global cybersecurity challenges from 2004 (the year of the GGE foundation) to 2023. It then identifies unsolved issues emerging from the GGE and OEWG, and finally reports and addresses the factors hindering further discussions on cybersecurity within those fora.

This research collected official documents, reports, and statements produced by the GGE and OEWG and their country members from 2004 to 2023. Particular attention has been dedicated to exploring the countries' divergent views on key cybersecurity issues, focusing especially on the applicability of international law, in particular the UN Charter principles, and international humanitarian law. Emphasis has been placed upon the 2004 and 2015 GGE as they failed to release consensus reports as a result of these divergent standpoints. In addition, as some scholars and policy-makers have reflected upon the contributions of the UN in the field of cybersecurity, the analysis of the work of the GGE and OEWG has been further supported by drawing upon academic sources. These sources have been particularly important to drive attention to the geopolitical contexts of each report of the GGE and OEWG and the turning points of the cybersecurity discussions.

REGULATING THE CYBERSPACE: GGE AND OEWG EFFORTS (2004-PRESENT)

ICTs and cybersecurity have been prominent matters on the UN's global agenda since 1998 when Russia first proposed a draft resolution in the First Committee of the UN General Assembly (UNGA) (Maurer, 2011: 20). In so doing, Russia claimed to be interested in developing "international law regimes for preventing the use of information technologies for purposes incompatible with missions of ensuring international stability and security" (Henderson, 2021: 584). On the other hand, Western countries showed concern that an international treaty could restrict freedom under the guise of enhancing information and telecommunications security (Henderson, 2021: 585), thereby demonstrating the suspicious approach that countries would take towards each other in discussions over cybersecurity. Despite these concerns, Russia introduced similar draft proposals over the years. Prompted by Russia, in 2002 the UNGA requested the Secretary-General to establish the UN GGE on Developments in the Field of Information and Telecommunications in the Context of International Security, marking a turning point in the UN's efforts on cybersecurity and confidence-building among states (Henriksen, 2019: 2).

The GGE became a discussion forum among a selected number of experts (15 to 25 members depending on the GGE session) based on equitable geographical distribution, tasked with submitting a consensus report on states' challenges and approaches to the use of ICTs (Ruhl et al., 2020: 4). Initially, the GGE's work was hindered by a lack of consensus among the participating states on key issues, including the applicability of IHL principles, such as the distinction principle, and international law to state behaviour in cyberspace (Schmitt, 2021). Moreover, as cyber attacks in the early 2000s were sporadic, decision- and policy-makers had a low awareness of cyber threats. Cyber operations also tended to stay out of the public eye and cybersecurity was generally seen as a technical issue to be addressed by IT departments and information security personnel (Tiirmaa-Klaar, 2021: 3).

However, the perception of the digital domain has significantly changed after the cyberattacks suffered by Estonia and Georgia in 2007 and 2008, respectively, which targeted critical infrastructures and created large-scale political and economic turmoil (Buckland, Schreier and Winkler, 2015: 24-28). This experience was crucial to raising global awareness about cybersecurity, and specifically to the role of the UN in leading discussions on this topic. Indeed, those cyber sieges "marked a starting point for cyber issues becoming increasingly mainstreamed to a more strategic level, both nationally and internationally" (Tiirmaa-Klaar, 2021: 4). Accordingly, the second UN GGE successfully issued, in July 2010, a report acknowledging that "[e]xisting and potential threats in the sphere of information security are among the most serious challenges of the twenty-first century" (United Nations, 2010).

Also essential to the success of the GGE was the new US administration under President Barack Obama (2009-2017), which changed the direction of the US cyber policy and pursued a cooperative approach with regard to Russia and the UN itself. This significant de-escalation between the US and Russia facilitated the reaching of the GGE goals and culminated in the US co-sponsoring, for the first time, a Russian draft resolution (Tiirmaa-Klaar, 2021: 9; Maurer, 2011: 23-24). Among the report's recommendations was a call for cooperation among states to develop confidence-building and capacity-building measures and further dialogue on norms pertaining to states' use of ICTs. Additionally, the risks associated with the employment of disruptive cyberattacks by non-state actors were addressed, albeit briefly, in the report (United Nations, 2010). The latter did not, however, clarify a number of outstanding legal issues (Henriksen, 2019: 2).

The UNGA set up a third GGE in December 2011 to discuss "norms, rules or principles of responsible behaviour of States" in cyberspace (Henriksen, 2019: 3). Its final report was issued in 2013 and recognised the applicability of international law, in particular the UN Charter, to cyberspace. Notably, the report highlighted state governance of ICTs-related activities and states' sovereignty over ICTs infrastructure located inside their borders (United Nations, 2013). Moreover, it stated the need for respect for human rights and fundamental freedoms in the digital space and highlighted the leading role the UN should play in promoting dialogue among countries, supporting confidence-building and capacity-building measures and regional efforts (United Nations, 2013).

Nevertheless, although the report acknowledged international law norms, participant states did not agree on how they should be applied to cyberspace in practical terms. For example, key international players such as China emphasised that applying IHL to ICTs would be very challenging as civilian and military targets are hardly discriminated against in cyberspace (Henderson, 2021: 603). In addition, some countries were more interested in discussing the creation of regulations for cybersecurity than the application of existing international law. In 2011, China, Russia, Tajikistan and Uzbekistan formed a backdrop to the meeting of the GGE and presented a draft of an International Code of Conduct for Information Security to the UNGA, attempting to provide further regulation to cyber-norms and governance. The draft, however, was not welcomed by countries like the US, who perceived its guidelines

as a justification for government control over internet resources. While there was little support for the draft, the GGE report acknowledged that additional norms could be developed over time (Henderson, 2021: 593-594).

The fourth GGE adopted a consensus report in July 2015. Although it did not clarify the applicability of international law to cybersecurity — like previous reports —, the fourth GGE addressed several important issues. Pawlak and Barmpaliou (2017: 128) highlight that the 2015 GGE report proposes voluntary and non-binding norms to prevent states from potentially using ICTs for illegal activities; forbids actions such as cyberattacks on critical infrastructures; and incentivise cooperation, for instance by assisting each other in the event of an attack. They also pointed to the progress in the discussions around capacity building, as the report introduced several measures to strengthen collaborative mechanisms (Pawlak and Barmpaliou, 2017: 128). Furthermore, although there is no explicit mention of the IHL in the report, it did make reference to the principles of "humanity, necessity, proportionality, and distinction" (United Nations, 2014), which are the key principles of this branch of international law.

The optimism characterising the 2015 GGE did not last long. The fifth GGE did not agree on a draft for a consensus report in 2017. The main challenge for the discussions was the main mission of the 2016-2017 GGE: establishing how international law should apply to the use of ICTs by states (Henderson, 2021: 598). While the US pushed for explicit statements on the issue, references to the right to self-defence, international law and IHL principles caused deep dissatisfaction among countries like Cuba (Glen, 2021: 1130). The Cuban representative emphasised his concern that states could intentionally legitimise punitive actions such as sanctions and the use of military force in the name of self-defence, thus disapproving the report's mentions of the law of armed conflict (Henderson, 2021: 3). As a result, the 2016-2017 UN GGE did not fulfil its mandate due to definitional disputes and further fundamental disagreements over interests and values (Glen, 2021: 1113).

In December 2018, the UNGA established two separate processes to discuss cybersecurity issues and norms in the period 2019-2021. Besides continuing with the work of the GGE, the UN also created the OWEG, following a Russia-sponsored resolution. Differently from the GGE, the OWEG has been open to all member States to discuss developments in ICTs (Henderson, 20221: 601). Both groups are mandated to work on the basis of international law, particularly the UN Charter, and "norms, rules and principles for the responsible behaviour of States" from the 2015 GGE report. Nonetheless, the OEWG's mandate is slightly broader and also examines whether possible changes to the regulations and additional rules of state behaviour are necessary. As aforementioned, this issue is a crucial source of contention between states in the cybersecurity dialogue. Whereas countries like Russia and China have sought to revise current norms and establish binding agreements that better serve their interests, the US and like-minded countries have ruled out any legal changes in previous discussions and argue this falls beyond the OWEG's mandate (Henderson, 2021: 602). Adding to the challenge of addressing the topic are some developing countries like India, Indonesia, and South Africa, which have not been active in the cyber norms debates (Basu, Poetranto and Lau, 2021). Therefore, the discussions on cybersecurity have been held back by both a lack of consensus and political will to resolve relevant issues.

The sixth and last GGE released its final report in 2021. The consensus on this report was commemorated by the international community especially because no agreement had been reached at the previous GGE. The Estonian Ambassador for Cyber Diplomacy, Heli Tiirmaa-Klaar (2021: 8) stated that "the report of the 2019–2021 GGE could be characterised as a rare victory of multilateral diplomacy." She explained that significant mentions of international law and attribution and explanations

of critical infrastructure protection norms satisfied Western countries. At the same time, the report addressed prominent issues raised by China, for example, creating a section on the ICTs supply chain (Tiirmaa-Klaar, 2021: 8). However, scholars also noted that debates over state sovereignty in cyberspace and the right to self-defence remained unsettled (Schmitt, 2021).

From 2019 to 2021, the OEWG worked in parallel with the last GGE. Its substantive sessions were considered a significant precedent for more inclusive debates on international cybersecurity because, besides the 193 countries involved, over 100 NGOs contributed to the discussions as observers (Hurel, 2022). The report issued in March 2021 reaffirmed the results of the previous GGE reports, including the applicability of international law, especially the UN Charter, to cyberspace. Regarding norms, the OEWG stated that they do not replace or modify states' compliance with international law but rather provide further guidance on responsible state behaviour in using ICTs (United Nations, 2021b). Moreover, as noted by Collett (2021), the report significantly advanced the development of principles and measures of ICTs capacity building.

In 2020 the UNGA renewed the OEWG's mandate for a five-year period (2021-2025). The mission of the OEWG remained unchanged, and its work has been divided into eleven substantive sessions, with a final report to be provided in 2025 (United Nations, 2021a). However, a turning point to this new mandate since 2022 has been the increasing geopolitical tension between the US and Russia in the context of the Russian war against Ukraine. Indeed, Ukraine has been suffering massive cyber intelligence operations and attacks by Russia, which have called the attention of policymakers and researchers concerned with the use of cyber capabilities to target critical infrastructures, including telecommunications, banking, transport, water supply and energy supplies (Willett, 2022; Levite, 2023).

Consequently, the war has also highlighted the debate on when cyber attacks cross the threshold to be legitimately considered acts of war, which the OEWG has found difficult to reach an international consensus on (Levite, 2023: 4). The increasing geopolitical tensions between Russia and Ukraine have also influenced the OEWG structure and participation. For instance, despite the OEWG's agreement on NGOs' involvement in the discussions, the participation of twenty-seven NGOs was opposed by Russia (Hurel, 2022). Similarly, Ukraine opposed the participation of Russian-based groups believed to have a relationship with the government (Pytlak and Acheson, 2022: 1). Moreover, opinions on the Annual Progress Report on the OEWG 2021-2025 drive attention to the little progress on critical issues also left unsolved by the GGE negotiations (Diplo Foundation, 2022).

Indeed, the OEWG has not reached an agreement on the applicability of international law principles such as the right to self-defence and IHL and on whether sovereignty is a principle or a rule in international law and whether new norms under an international cyber convention are necessary (Basu, Poetranto and Lau, 2021). Furthermore, the OEWG has not agreed, not even among Western countries, on whether sovereignty is a principle or a rule in international law. For example, in an analysis of the OEWG meeting in February 2020, Roguski (2020) explains that certain countries like the United Kingdom believe that sovereignty is merely an established principle of international law and does not in itself create independent legal obligations. Rather, sovereignty is protected by other well-established principles of international law, such as the prohibition of using force or the principle of non-intervention. Other nations, such as France, Germany, and the Netherlands, however, support the sovereignty-as-a-rule principle and argue that, under certain circumstances, a cyber operation may also breach the sovereignty of a targeted country (Roguski, 2020). Hence, despite the intense efforts of the UN since 2004, the progress on cybersecurity has been hindered by fundamental disagreements between states and difficulties in norms interpretations and applicability.

THE UN CHARTER IN CYBERSPACE

The GGE's and OEWG's reports and the related UNGA resolutions acknowledge that the UN Charter applies in its entirety to cyberspace. However, there has not been a consensus on procedures and modalities. In particular, its applicability is challenging regarding specific articles (Glen, 2021: 1128-1131). One of the core principles of the UN Charter is self-determination and the equality of states (Article 2), which, therefore, entails states' jurisdiction over ICTs within their territory. As shown in the GGE's and OEWG's reports, states have an obligation to respect the sovereignty of other countries and refrain from activities that could violate this principle. Nevertheless, states like Russia and China have used the sovereignty principle to justify their intense control over internal cyber activities, claiming to be fighting against external threats (Glen, 2021: 1132).

As aforementioned, in the context of the third meeting of the GGE in 2011, China, Russia, Tajikistan and Uzbekistan submitted to the UNGA an International Code of Conduct for Information Security to provide further regulations concerning cyber-norms and governance. The Code suggested that "policy authority for Internet-related public issues is the sovereign right of States, which have rights and responsibilities for international Internet-related public policy issues" (United Nations, 2011), attempting to legitimise limitations of the freedom of expression in the digital space. Over the years, China has widely advocated for the acceptance of the 'information sovereignty' concept, thus concentrating on information security – i.e. protecting state authority over information – rather than cyber security (Kiyan, 2021). Notably, during the 2015 World Internet Conference in China, Chinese President Xi Jinping spoke out against "internet hegemony" and "foreign interference in [China's] internal affairs through the Internet" (Basu, Poetranto and Lau, 2021).

Whereas states like China interpret the UN principle of sovereignty as countries' non-interference in other states' cyber activities, others emphasise it as a responsibility to prevent actors from using their territory to conduct malicious digital activities. This aspect, promoted primarily by Western countries, has resulted in norms on GGE and OEGW reports to address the use of proxies in cyber operations (Digital Watch, 2023). Nonetheless, even among Western countries, there are diverging interpretations as to whether sovereignty should be addressed as a principle of international law or a rule (Roguski, 2020), as explained previously. Besides the different understanding of sovereignty in cyberspace, the violation of this principle has also become more complex to verify in the cyber-ecosystem. In this regard, it is important to note that cyberattacks targeting extraterritorial data storage, for instance, frequently include proxy servers or other tools that make the attackers undetectable. Hence, determining whether they are involved in a cross-border activity that would violate a state's sovereignty can be quite challenging (Digital Watch, 2023).

The non-interference principle, which stems from the UN principle of sovereignty, is also challenged in cyberspace. Emerging and disruptive technologies allow states to interfere in others' affairs without the (physical) use of force. For instance, a cyberattack can severely damage a country by attacking its financial industry without the need to target a military or governmental asset (Buckland, Schreier and Winkler, 2015: 25). Accordingly, it is incredibly challenging for UN members to agree on what cyber operations should be considered coercion, use of force, or an armed attack (Digital Watch, 2023). Moreover, international law does not clearly define the use of force and coercion in Art. 2(4) of the UN Charter — for example, coercion as economic, diplomatic, and political pressure is not defined in the article (Digital Watch, 2023). Such clarifications and consensus among UN members are particularly important due to potential extensive cyberattacks against critical infrastructure, like the ones suffered by Estonia, Georgia, and Ukraine. Yet, applying the non-interference principle in cyberspace and

agreeing on common criteria for forms of aggression between states highly depends on the political will of states. As noted by Levite (2023: 4-5), this lack of common criteria also originates from the latitude that some states want to have to interpret their adversaries' offensive cyber operations on a case-by-case and to undertake such actions themselves. For instance, the US and Israel's cyber operations against the Iranian nuclear programme were considered legitimate and legal in non-war settings by the US and Israel, although they were both intended to cause damage and were in violation of the non-interference principle (Levite, 2023: 5). Therefore, this attitude has hindered the progress of UN discussions around state-responsible behaviour and confidence-building measures.

The applicability of Article 51 of the UN Charter in cyberspace is also still being determined. The right to self-defence is difficult to assess in cyber operations because the origin of the threat is often hard to identify. Hence, traditional deterrence and response policies are undermined. In current discussions on cybersecurity, it is also unclear how a state could use its right to self-defence even if an attacker is identified correctly (Buckland, Schreier and Winkler, 2015: 24-25). Indeed, the disagreement over the means a country could employ to respond to major cyberattacks was one of the main reasons why the GGE 2017 failed to issue a consensus report. Whereas NATO confirms that under its Art. 5, member countries can respond to a cyberattack by any means, including conventional means of warfare (Stoltenberg, 2019), this is not a resolved issue within the UN discussions on cybersecurity. OEWG members like Russia, Cuba, and China do not acknowledge the use of force as a legitimate reaction to cyberattacks, at least not without the approval of the UNSC and in accordance with the UN Charter (Glen, 2021: 1130-1131). While these countries' position also reflects their national interests, the risk of states justifying armed attacks as a response to cyberattacks is indeed a risk to international peace. Hence, the applicability of the UN Charter further needs clarification, as do mechanisms to support the identification of threats and attackers efficiently.

INTERNATIONAL HUMANITARIAN LAW AND CYBERSPACE

The issue of whether IHL should apply to cyberspace has been particularly challenging in UN discussions. In OEWG negotiations, Cuba argued that incorporating IHL would normalise the militarisation of cyberspace and legitimise cyber wars (Basu, Poetranto and Lau, 2021) and that the group should focus on the prevention of armed conflict rather than the applicability of such a particular principle (Achten, 2019). As previously mentioned, China also raised concerns about the applicability of IHL, especially the principle of distinction, emphasising the challenges to distinguish between civilian and military targets in cyberspace. Although the bulk of the observers does not find a direct connection between the militarisation of cyberspace and the recognition of IHL applicability, this has been a long-standing point made by Chinese experts and has further hindered discussions of international law in many GGEs (Tiirmaa-Klaar, 2021: 6). Western countries, on the other hand, have argued that IHL – and the right to self-defence – should be applied to cyberspace (Henderson, 2021: 603).

The applicability of IHL is a prominent issue in light of the growing capacity of states to develop offensive cyber capabilities with high potential human costs, such as attacks on critical infrastructures. For instance, just a few months after the 2015 GGE report was adopted, hackers tied to Russia utilised technology to take out the Ukrainian power grid, leaving residents without electricity for about seven hours (Basu, Poetranto and Lau, 2021). It is worth noting, however, that there is consensus, at least among Western countries, on the applicability of IHL to cyber operations in the context of armed conflicts. The International Committee of the Red Cross also acknowledges that IHL applies to all cyber operations occurring within an armed conflict (ICRCa, 2022). Therefore, more attention should be given to

"how IHL governs cyber operations during an armed conflict, whether international or non-international" (Schmitt, 2021). In this regard, the lack of a clear definition of what constitutes an armed attack or merely an attack is a significant issue in international law, which also compromises the applicability of IHL in the digital space. Currently, there is no consensus as to whether an attack entails injury, death, damage or destruction or a loss of functionality in critical infrastructures (Khawaja, 2022). Similarly, the international system has not yet agreed on what would constitute the start of an armed conflict, especially when cyberattacks are employed in isolation — without the use of kinetic force (Ramluckan, 2020: 103). What would represent an act of war also remains contentious. For example, while the 2014 attacks on Ukrainian energy systems were a cyber operation targeted at critical infrastructure with negative effects on the population, at the time this was not considered to cross the threshold of war (Levite, 2023: 4). This event shows that despite the UN's efforts to make states agree on these key definitions and consequently the applicability of the IHL to protect civilians, some states are reluctant to cooperate as they benefit from the blurred lines between legitimate and illegitimate peacetime operations.

Besides the diverging ideas of countries concerning IHL in cyberspace, it is also important to mention the practical challenges of the law's application. As pointed out by China, it can indeed be difficult to apply the distinction principle. Moreover, the so-called attribution problem in cyberspace also prevents the successful applicability of IHL. As noted by Hollis (2021), identifying the origins of malicious behaviour is difficult and time-consuming. The reliance of states upon proxies is a further challenge to attribution and accountability as there is a need to prove states' control over the proxy actors and the attackers can use plausible deniability as a defence. Also, deception may be employed, such as redirecting the assault so that it appears to have originated from an incorrect location (Ramluckan, 2020: 3). Consequently, holding states accountable for IHL violations, that is, fully applying the IHL cardinal principles in cyberspace, is a complex issue, still to be adequately addressed by OEWG countries (Khawaja, 2022).

NEXT STEPS IN REGULATING CYBERSPACE

The debate on international law applicability to cyberspace and the implementation of new norms constitute key issues for the international community of states. They are, ultimately, an attempt to reconcile divergent strategic interests and opposing worldviews. The outcomes of such debates, as argued by Henriksen (2019: 4), will determine how countries use ICTs to pursue their foreign policy objectives. Indeed, the challenges previously addressed have paved the way for states like Russia to argue that current international norms are insufficient to regulate cyber activities and propose, over the years, the creation of a cyber convention (Maurer, 2011: 21). Scholars have suggested that Russia and China have strategically pushed for the creation of new norms that could further control prospects of a 'cyber arms race' and counter the US dominance over ICTs (Henriksen, 2019: 4). However, such proposals have been received by the US and like-minded countries with strong scepticism as a treaty on cybersecurity could be used to limit the freedom of information under the guise of increasing ICT's security (Maurer, 2011: 21). Instead, most OEWG representatives have shown interest in further exploring legal regulations and norms for the cyber environment and their implementation to achieve cybersecurity (Henderson, 2021: 603-604). Notably, the US has stood against any norm proposal that could limit its cyber capabilities, relying on international law to maintain its superior position and to prevent other states from engaging in what the country perceives as disruptive activities (Henriksen, 2019: 4).

The debate on the implementation of new cyber norms has been revived recently. In March 2023, Russia submitted its vision for a Convention of the

UN on Ensuring International Information Security to the OEWG. This document illustrates Russia's resistance to engage in discussions on the international law principles in cyberspace. Instead, it proposes new norms to better shape the international system according to Russian values and interests.

On top of the "Main threats to international information security," a section written with contributions from China and Iran, Russia calls for sovereign equality, the territorial integrity of states and non-interference in the internal affairs of others through any cyber operation (Russian Federation, 2023). Moreover, Weber (2023) has noted that the document merely mentions freedom of expression without further expanding on human rights and calls for the possibility of it being restricted if necessary. Another proposal that further reveals Russia's interests is the establishment of institutional mechanisms to ensure de-anonymisation in cyberspace, potentially to legitimise domestic surveillance (Weber, 2023). Although this has been a consistent position of Russia throughout the years, due to its ongoing war against Ukraine, the attitute can also be interpreted as a policy strategy to keep control over Russia's domestic cyberspace and prevent any external reaction to the war. Indeed, since the beggining of the aggression, Russia has weaponised cyber governance by blocking several news websites and social media platforms, for example, to constrain access to information about the war (Meinel and Hagebölling, 2023). This attitude, therefore, will likely hinder progress on ongoing cybersecurity discussions at the UN level. The reactions to the Convention, however, are expected to be clarified in July 2023 during the OEWG's third substantive session (United Nations, 2021).

CONCLUSIONS

This article shows that the UN's efforts to regulate cyberspace in accordance with international law and promote ethical and responsible state behaviour have been challenged by key participating states, which have rather focused on protecting their vnational interests. It uses official documentation, reports, and statements produced by the GGE and OEWG and their member countries from 2004 to 2023 to explore those bodies' contributions to cybersecurity discussions and their remaining challenges. As the OEWG's mandate is ongoing, this article provides an analysis of the UN efforts in cybersecurity until June 2023 only. Moreover, as the UN's involvement in cybersecurity is still an under-explored topic by academia, this article is limited by a scarce number of scholarly sources.

The analysis of the discussions and reports from the GGE and OEWG reveals that great powers such as Russia, China, and the US, have not agreed on international regulations as they aim to constrain each other's cyber capabilities, while also preserving their sovereign control over their domestic cyber-ecosystem. In particular, Russia has widely advocated for a cyber convention that would better align with its goals of control over information within its borders, posing a great challenge to freedom of expression and human rights. Furthermore, great powers have tried to keep benefiting from the blurred lines between war and peace to deploy their cyber capabilities when convenient to their national interests. Diverging standpoints of states have also hindered the UN's efforts, leading to different interpretations of the UN Charter principles, thus holding states back from agreeing on a common approach to cyber activities. As argued, applying these principles to cyberspace is also difficult due to unclear definitions of key terms such as what would constitute coercion, use of force, and armed attack. Consequently, the application of IHL has become a challenge for states to address since attribution and accountability in the cyber-ecosystem are even more difficult to verify.

Yet, this article also acknowledges that the GGE and OEWG have made significant contributions to cybersecurity and, therefore, can be considered a success in UN efforts to shape state behaviour in cyberspace, as well as confidence and capacity-building measures among its member states.

Especially because the OEWG involves all the UN member states, its discussions fora have been an opportunity for countries to express their concerns to the international community. Therefore, further research on the UN's involvement in cybersecurity, particularly the OEWG's current mandate, is essential to deepen academics' and policymakers' understanding of states' behaviour in this emerging field, which includes complex elements of competition and cooperation based on states' national interests. Especially due to Russia's approach to cyberspace amidst its war against Ukraine, the discussions on cybersecurity at the UN level should be watched attentively by the international community in the years to come.

BIBLIOGRAPHY

Achten, N. (2019). 'New U.N. Debate on Cybersecurity in the Context of International Security'. [online] *Lawfare*. Available at: https://www.lawfareblog.com/new-un-debate-cybersecurity-context-international-security [Accessed 25 Apr. 2023].

Basu, A, Poetranto, I. and Lau, J. (2021). 'The UN Struggles to Make Progress on Securing Cyberspace'. [online] *Carnegie Endowment for International Peace*. Available at: https://carnegieendowment.org/2021/05/19/un-struggles-to-make-progress-on-securing-cyberspace-pub-84491 [Accessed 24 Apr. 2023].

Buckland, B.S., Schreier, F. and Winkler, T.H. (2015). 'Democratic Governance Challenges of Cyber Security'. [online] *DCAF | Geneva Centre for Security Sector Governance*, DCAF, 24–28. Available at: https://www.dcaf.ch/democratic-governance-challenges-cyber-security [Accessed 25 Apr. 2023].

Collett, R. (2021). 'Understanding cybersecurity capacity building and its relationship to norms and confidence building measures'. *Journal of Cyber Policy* 6(3), 1–20. doi:https://doi.org/10.1080/23738871.2021.1948582.

CSIS (2022). 'Significant Cyber Incidents'. [online] *CSIS | Center for Strategic & International Studies*. Available at: https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents [Accessed 16 Apr. 2023].

Digital Watch (2023). 'UN OEWG in 2023 - DW Observatory'. [online] *Geneva Internet Platform DigWatch*. Available at: https://dig.watch/processes/un-gge#The-current-process---OEWG-2021-2025 [Accessed 25 Apr. 2023].

Diplo Foundation (2022). 'What's new with cybersecurity negotiations: The OEWG 2021–2025 annual report adopted' - Diplo. [online] *DIPLO*. Available at: https://www.diplomacy.edu/blog/whats-new-with-cybersecurity-negotiations-the-oewg-2021-2025-annual-report-adopted/ [Accessed 20 Apr. 2023].

Glen, C.M. (2021). 'Norm Entrepreneurship in Global Cybersecurity'. *Politics & Policy* 49(5), 1128–1131. doi:https://doi.org/10.1111/polp.12430.

Henderson, C. (2021). 'The United Nations and the regulation of cyber-security'. In: N. Tsagourias and R. Buchan, eds., *Research Handbook on International Law and Cyberspace*. [online] Cheltenham: Edward Elgar Publishing Limited, 583–604. Available at: https://doi.org/10.4337/9781782547396.00035 [Accessed 12 Apr. 2023].

Henriksen, A. (2019). 'The end of the road for the UN GGE process: The future regulation of cyberspace'. *Journal of Cybersecurity* 5(1), 2–4. doi:https://doi.org/10.1093/cybsec/tyy009.

Hollis, D. (2021). 'A Brief Primer on International Law and Cyberspace'. [online] *Carnegie Endowment for International Peace*. Available at: https://carnegieendowment.org/2021/06/14/brief-primer-on-international-law-and-cyberspace-pub-84763 [Accessed 25 Apr. 2023].

Hurel, L.M. (2022). 'The Rocky Road to Cyber Norms at the United Nations'. [online] *Council on Foreign Relations*. Available at: https://www.cfr.org/blog/rocky-road-cyber-norms-united-nations-0 [Accessed 23 Apr. 2023].

ICRC (2022a). 'Cyberspace is not a legal vacuum, including during armed conflict'. [online] *ICRC | International Committee of the Red Cross*. Available at: https://www.icrc.org/en/document/cyberspace-not-legal-vacuum-including-during-armed-conflict [Accessed 19 Jun. 2023].

ICRC (2022b). 'What is international humanitarian law?' [online] *International Committee of the Red Cross*. Available at: https://www.icrc.org/en/document/what-international-humanitarian-law [Accessed 20 Jun. 2023].

Khawaja, A.A. (2022). Cyber Warfare and International Humanitarian Law. [online] DLP Forum. Available at: https://www.dlpforum.org/2022/08/17/cyber-warfare-and-international-humanitarian-law/ [Accessed 25 Apr. 2023].

Kiyan, O. (2021). 'Establishing Cybersecurity Norms in the United Nations: The Role of U.S.-Russia Divergence'. [online] *Harvard International Review*. Available at: https://hir.harvard.edu/establishing-cybersecurity-norms-in-the-united-nations-the-role-of-u-s-russia-divergence/ [Accessed 25 Apr. 2023].

Levite, A.E. (2023). 'Integrating Cyber Into Warfighting: Some Early Takeaways From the Ukraine Conflict'. [online] *Carnegie Endowment for International Peace*. Available at: https://carnegieendowment.org/2023/04/18/integrating-cyber-into-warfighting-some-early-takeaways-from-ukraine-conflict-pub-89544 [Accessed 20 Jun. 2023].

Maurer, T. (2011). 'Cyber Norm Emergence at the United Nations —An Analysis of the UN's Activities Regarding Cyber-security'. *Science, Technology, and Public Policy Program*. Belfer Center, 20.

Meinel, C. and Hagebölling, D. (2023). 'Russia's War Against Ukraine is Catalyzing Internet Fragmentation'. [online] *Council on Foreign Relations*. Available at: https://www.cfr.org/blog/russias-war-against-ukraine-catalyzing-internet-fragmentation [Accessed 23 Jun. 2023].

Pawlak, P. and Barmpaliou, P.-N. (2017). 'Politics of cybersecurity capacity building: conundrum and opportunity'. *Journal of Cyber Policy* 2(1), 128. doi:https://doi.org/10.1080/23738871.2017.1294610.

Pytlak, A. and Acheson, R. eds., (2022). 'Cyber Peace & Security Monitor'. [online] *Reaching Critical Will* 1. Available at: https://www.reachingcriticalwill.org/disarmament-fora/ict/oewg-ii/cyber-monitor/16310-cyber-peace-security-monitor-vol-2-no-7 [Accessed 18 Apr. 2023].

Ramluckan, T. (2020). 'International Humanitarian Law and its Applicability to the South African Cyber Environment'. *Journal of Information Warfare* [online] 19(3), 103–106. Available at: https://www.jstor.org/stable/27033635 [Accessed 20 Jun. 2023].

Roguski, P. (2020). 'The Importance of New Statements on Sovereignty in Cyberspace by Austria, the Czech Republic and United States'. [online] *Just Security*. Available at: https://www.justsecurity.org/70108/the-importance-of-new-statements-on-sovereignty-in-cyberspace-by-austria-the-czech-republic-and-united-states/ [Accessed 20 Jun. 2023].

Ruhl, C., Hollis, D., Maurer, T. and Hoffman, W. (2020b). 'Cyberspace and Geopolitics: Assessing Global Cybersecurity Norm Processes at a Crossroads'. [online] *Carnegie Endowment for International Peace* 4. Available at: https://www.jstor.org/stable/resrep24286?searchText=&searchUri=&ab_segments=&refreqid=&searchKey= [Accessed 24 Jun. 2023].

Russian Federation (2023). 'Updated Concept of the Convention of the United Nations on Ensuring International Information Security'. [Online] Available at: https://docs-library.unoda.org/OpenEnded_Working_Group_on_Information_and_Communication_Technologies__(2021)/ENG_Concept_of_UN_Convention__on_International_Information_Security_Proposal_of_the_Russian__Federation_0.pdf [Accessed 23 Apr. 2023].

Schmitt, M. (2021). 'The Sixth GGE and International Law in Cyberspace'. [online] *Just Security*. Available at: https://www.justsecurity.org/76864/the-sixth-united-nations-gge-and-international-law-in-cyberspace/ [Accessed 20 Apr. 2023].

Stoltenberg, J. (2019). 'NATO will defend itself' (Article by NATO Secretary General Jens Stoltenberg published in *Prospect*). [online] *NATO*. Available at: https://www.nato.int/cps/en/natohq/news_168435.htm?selectedLocale=en [Accessed 20 Apr. 2023].

Tiirmaa-Klaar, H. (2021). 'The Evolution of the UN Group of Governmental Experts on Cyber Issues: From a Marginal Group to a Major International Security Norm-Setting Body'. [online] *Hague Centre for Strategic Studies*, 3–9. Available at: https://www.jstor.org/stable/resrep38747 [Accessed 20 Apr. 2023].

United Nations (2010). Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security: Note by the Secretary-General. [Online] A/65/201. Available at: https://digitallibrary.un.org/record/688507 [Accessed 19 Apr. 2023].

United Nations (2013). 'Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security: Note by the Secretary-General'. [Online] A/68/98. Available at: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N13/371/66/PDF/N1337166.pdf?OpenElement [Accessed 21 Apr. 2023].

United Nations (2014). 'Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security: Note by the Secretary-General'. [Online] A/70/174. Available at: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N15/228/35/PDF/N1522835.pdf?OpenElement [Accessed 20 Apr. 2023].

United Nations (2011). 'Letter dated 12 September 2011 from the Permanent Representatives of China, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General'. [Online] A/66/359. Available at: https://digitallibrary.un.org/record/710973#record-files-collapse-header [Accessed 20 Apr. 2023].

United Nations (2021a). 'Open-ended working group on information and communication technologies (2021)' [Online] *United Nations | Office for Disarmament Affairs*. Available at: https://meetings.unoda.org/open-ended-working-group-on-information-and-communication-technologies-2021 [Accessed 20 Apr. 2023].

United Nations (2021b). 'Open-ended working group on developments in the field of information and telecommunications in the context of international security: Final Substantive Report'. [Online] A/AC.290/2021/CRP.2. Available at: https://daccess-ods.un.org/access.nsf/Get?OpenAgent&DS=A/AC.290/2021/CRP.2&Lang=E [Accessed 24 Apr. 2023].

United Nations (2021c). 'Our Common Agenda - Report Of The Secretary -General'. S.L.: United Nations.

United Nations (2022). 'International Law and Justice'. [online] *United Nations*. Available at: https://www.un.org/en/global-issues/international-law-and-justice [Accessed 20 Jun. 2023]

Weber, V. (2023). 'The Dangers of a New Russian Proposal for a UN Convention on International Information Security'. [online] *Council on Foreign Relations*. Available at: https://www.cfr.org/blog/dangers-new-russian-proposal-un-convention-international-information-security [Accessed 25 Apr. 2023].

Willett, M. (2022). 'The Cyber Dimension of the Russia–Ukraine War'. *Survival* 64(5), 7–26. doi:https://doi.org/10.1080/00396338.2022.2126193.