The impact of the practice of international organizations on the United Nations recent works on cybersecurity

di Andrea Insolia

Title: L'influenza della prassi delle organizzazioni internazionali nei recenti lavori dell'ONU sulla cybersicurezza

Keywords: United Nations; OEWG; Cyberspace; African Union; European Union; Inter-American Juridical Committee.

1. – The constant increase malicious cyber-operations by States and non-State actors, as well as their frequent use in traditional an hybrid conflicts, alone or in combination with conventional weapons (see the Report of the first Open-Ended Working Group on Security of and in the Use of Information and Communications Technologies (OEWG, 2019-2021), A/75/816, 18 March 2021, Annex I, para 16; see also the current OEWG's (2021-2025) *Draft Final Report of the Open-Ended Working Group on Security of and in the Use of Information and Communications Technologies 2021–2025, Submitted to the 80th Session of the General Assembly pursuant to General Assembly Resolution 75/240*, 23 May 2025, paras 16 and 21, hereinafter "Draft Final Report", available here: meetings.unoda.org/meeting/57871/documents), which also increasingly target directly international organizations (IOs), has prompted a growing number of them to address the phenomenon both through the convening of working groups of independent or governmental experts in the field of information and telecommunication technologies (ICT) and through the adoption of common positions on the applicability of certain fundamental principles and norms of international law to State activities in cyberspace.

In addition to the long-standing work of the United Nations (UN) and UN-based organisms, several other regional organizations, in a very similar way to what many States have done, have either adopted (common) positions on the applicability of international law to cyberspace (e.g. NATO, *Allied Joint Doctrine for Cyberspace Operations*, 2020; African Union Peace and Security Council, *Common African Position on the Application of International Law to the Use of Information and Communication Technologies in Cyberspace*, 2024; Council of the European Union *Declaration on a Common Understanding of International Law in Cyberspace*, 2024), or conducted studies on ICT security and international law through organs of experts, in consultation with Member States (e.g. the Inter-American Juridical Committee of the Organization of American States, *Second Report on International Law applicable to Cyberspace*, CJI/doc. 671/22 rev.2 corr.1, 21 October 2022).

This growing practice is increasingly raising the attention of scholars (see, recently, the contributions in P. Gargiulo, D. Giovannelli, A.L. Sciacovelli (Eds), *Cybersecurity Governance and Normative Frameworks: Non-Western Countries and International Organizations Perspectives*, in Quaderni de *Com. Internaz.*, n. 29, 2024, esp. p. 203 ff.).

The present contribution will briefly comment upon one such development. Firstly, the upcoming completion, in July 2025, of the second OEWG (established pursuant to UN General Assembly resolution 75/240) provides the opportunity to reflect upon the achievements of the twenty-year working groups experience within the UN system.

This will be done by discussing, on the one hand, the progress made by the current OEWG on the issue of whether and how international law applies in cyberspace, as it emerges from the recently released Zero-Draft of the current OEWG's *Draft Final Report* quoted above, to be adopted in its eleventh and final substantive session in July 2025. The *Draft Final Report* will be put into perspective by reviewing also previous reports of the same and other groups of governmental experts within the UN. In fact, these reports are to be understood as part of a "cumulative and evolving framework for responsible State behavior in the use of ICTs" and have formed the basis for the discussions within the current and former OEWGs. (*Draft the Final Report*, 23 May 2025, para. 5).

This will allow an assessment of the achievements of the working groups negotiating format on this fundamental question, after twenty-years of work. On the other hand, the current OEWG's perspective will rapidly be compared with that of several regional organizations that have recently adopted (common) positions or declarations on how international law applies in cyberspace.

Secondly, the OEWG's proposal for the establishment of an "Open-Ended Action-Oriented Permanent Mechanism on ICT Security in the context of international security" will be briefly discussed (see the current OEWG's *Third Annual Progress Report*, 22 July 2024, UN Doc. A/79/214, Annex C), which was "welcomed" by the General Assembly in December 2024 (see UNGA resolution 79/237).

2. – Since the end of the 1990s, the United Nations started addressing the use of ICT technologies by both State and non-State actors, the international rules and principles applicable to it, and the implications for the maintenance of international peace and security (see generally C. Henderson, *The United Nations and the regulation of cyber-security*, in N. Tsagourias, R. Buchan (Eds), Research Handbook on International Law and Cyberspace, Elgar Publishing, 2021, p. 582 ss.; I. Brunner, 1998: UNGA Resolution 53/70 'Developments in the Field of Information and Telecommunications in the Context of International Security' and Its Influence on the International Rule of Law in Cyberspace, available here: papers.ssrn.com/sol3/papers.cfm?abstract_id=3856900; P. Gargiulo, *The United Nations and Cybersecurity*, in P. Gargiulo, D. Giovannelli, A.L. Sciacovelli (Eds), op. cit., p. 203 ss.). However, as is known, ever since the adoption of General Assembly resolution 53/70 of 1999, sponsored by Russia, the activity of different UNGA Committees and of several consecutive working groups of governmental experts has been marked by fundamental differences between Eastern and Western States concerning issues such as freedom of information, whether the focus should be on cybercrime or on the use of ICTs to conduct attacks against the sovereignty of other States and, most notably, whether existing international law is applicable to State activities in cyberspace or whether new rules and principles need to be developed and internationally agreed upon in a legally binding framework on ICTs

(see how this difference is still being reiterated in the Final Report of the First OEWG, 18 March 2021, A/75/816, p. 19, para 16).

Indeed, the latter view, advocated most prominently by Russia and China, already underpinned resolution 53/70, which invited all Member States to inform the Secretary-General of their views and assessments on, among other things, the "[a]dvisability of *developing* international principles that would enhance the security of global information and telecommunications systems and help to combat information terrorism and criminality". On the contrary, the United States, EU States, as well as several others, have consistently maintained – with some variations – that existing international law applicable to the use of traditional (or kinetic) weapons applies also, *mutatis mutandis*, to States' behavior in cyberspace, and have endeavored to direct the debate within these working groups to focus on the question of *how* such rules and principles applies in cyberspace, admittedly without much success.

This fundamental difference helps explaining, on the one hand, the somewhat disappointing outcome, at least on this specific point, of several of these working groups – save for the, by now, distant occasions in which the views of the Western and Eastern "blocs" have aligned –, and the consequent decision to shift their focus in subsequent reports on the development of voluntary, non-binding norms of responsible State behavior in cyberspace as well as of confidence-building, international cooperation and capacity-building measures on ICT security. On the other, this situation has caused a "splintering" in the negotiation process within the UN. After five consecutive and limited composition groups of Governmental Experts on Advancing Responsible State Behavior in Cyberspace in the Context of International Security (GGE, the first of which was established in 2004), the failure of the Fifth GGE to adopt its consensus report in 2017, generated a call for a more inclusive and transparent negotiation framework which ultimately prompted the establishment, in parallel to the Sixth and final GGE (2019-2021) of the already mentioned First OEWG (2019-2021), open to all UN member States and entrusted with a partially overlapping, but wider, mandate.

A brief overview of the work and outcomes of previous working groups of governmental experts may be useful to properly assess the *Draft Final Report* of the current OEWG and put into perspective the overall working groups negotiating format over the course of a little more than 20 years.

2.1. – As mentioned, international law was almost completely absent from the first (2004-2005) and second (2009-2010) GGE's Reports. These groups, while certainly raising the attention on ICT issues in the international agenda, were unable to adopt a consensus report focusing on international law, precisely because of "significant differences on key aspects of international information security" (E. Tikk-Ringas, *Developments in the FielD oF inFormation anD telecommunication in the context oF international security: Work of the UN first Committee 1998-2012*, ICT4Peace Publishing, Geneva, 2012, p. 7, available here: www.files.ethz.ch/isn/167403/Eneken-GGE-2012-Brief.pdf), given also the lack, at that time, of unified and commonly accepted definitions of key terms and concepts, and of "differing interpretations of current international law in the area of international information security" (Ambassador A.V. Krutskikh, UNGA Verbatim Record (17 October 2005) UN Doc A/C.1/60/PV.13, pp. 3-5, at 5). The Second GGE's Report, in fact, mostly ignored international law issues, merely underscoring the uncertainties regarding attribution of cyber-attacks and, most eloquently, the "lack of shared understanding regarding international norms pertaining to State use of ICTs", as factors raising the risk of instability and misperception, and hinted to the possibility that "[g]iven the unique attributes of

ICTs, additional norms could be developed over time" (UN Doc. A/65/201, 30 July 2010, p. 7, paras 7, 14).

It was only with the Third (2012-2013) and, more comprehensively, Fourth (2014-2015) GGEs' Reports that significant results were achieved in this respect. The Third Report acknowledged for the first time the applicability of international law and of the UN Charter in particular, underlining their importance for maintaining peace and stability and promoting an open, secure peaceful and accessible ICT environment. It further acknowledged the applicability in cyberspace of State sovereignty and of the norms and principles flowing from it, as well as of human rights and obligations deriving from the commission of internationally wrongful acts, if attributable to a State. It did not, however, expand further on *how* these, and possibly other, norms and principles apply such activities, pointing out that "[c]ommon understandings on how such norms shall apply to State behavior and the use of ICTs by States requires further study" (UN Doc. A/68/98, 24 June 2013, p. 8, paras 16, 19-23).

The Fourth GGE's Report (UN Doc. A/70/174, 22 July 2015) is, to this day, the most significant document produced within the UN system on the specific question of whether and how international law applies in cyberspace. The Report contains two distinct sections that address directly or indirectly these issues. Under heading III of the Report, the Group laid down a non-exhaustive list of 11 voluntary, non-binding norms and principles of responsible State behavior in cyberspace, subsequently endorsed and recommended by the General Assembly together with the report (UNGA res. 71/28, 9 December 2016, and 73/27, 11 December 2018, para. 1). These were initially proposed by the United States in reaction to the revised *International Code of Conduct for Information Security* previously submitted by China, Kazakhstan, Kyrgyzstan, Russia, Tajikistan and Uzbekistan, and drafted within the framework of the Shanghai Cooperation Organization (UN Doc. A/69/723; a previous version had been submitted in 2013, see Henderson, op. cit., pp. 593-594; E. Korzak, *The 2015 GGE Report: What Next for Norms in Cyberspace?*, *Lawfare*, 23 September 2015, available here: www.lawfaremedia.org/article/2015-gge-report-what-next-norms-cyberspace). They are to be intended as compatible with – and, indeed, restate and clarify, in hortatory terms – some of the principles and rules of international law enshrined in the UN Charter and stated in more detail under heading VI of the Report, entitled "How international law applies to the use of ICTs" (A/70/174, cit., p. 12, para. 24 ff.).

Under this heading the 2015 Report stated, firstly, that the UN Charter is applicable "in its entirety". Secondly, it acknowledged the applicability of the principles of State sovereignty, sovereign equality, and non-intervention in the internal affairs of other States; of peaceful settlement of international disputes and of the prohibition of the threat or use of force, of respect for human rights and fundamental freedoms. It further "noted" the principles of humanity, necessity, proportionality and distinction. Still, the Report did not expand on how these rules and principles apply in cyberspace and could not achieve the desired level of clarity on some of the most contentious issues, i.e. self-defense, countermeasures, attribution, and international humanitarian law.

As will be discussed in more detail below, further clarifications were however offered on some of these issues in the subsequent 2021 GGE () and First OEWG reports (A/75/816), as well as in the current OEWG reports (*Third Annual Progress Report*, A/79/214; *Draft Final Report*, cit.). Which will be discussed below.

2.2. – Starting with self-defense, while the 2015 Report acknowledged the applicability of the UN Charter "in its entirety", it then merely noted, e.g., "the inherent right of States to take measures consistent with international law and as

recognized in the Charter" and restated the need for further study on the matter (A/70/174, cit., para. 28(c)). This may certainly be intended as an implicit reference to self-defense. However, no mention was made in that Report to the specific issues raised by its application to cyber activities, such as the very notion of (cyber) armed-attack, the means (cyber and/or kinetic) through which a reaction in self-defense may be carried out, the requirements of necessity, proportionality and immediacy, or the problem of self-defense against non-State actors (all particularly problematic given the peculiarities of cyber-attacks). The existence, in this and other respects, of substantial disagreement between States is shown by the failure of Fifth GGE to adopt a consensus report altogether. Russia, China and Cuba, while restating in general terms the applicability of international law to cyberspace, declared their serious concern over the pretension "to convert cyberspace into a theater of military operations" and legitimize "unilateral punitive force actions, including the application of sanctions and even military action by States claiming to be victims of illicit uses of ICTs". Criticism was particularly addressed at paragraph 34 of the draft final report, which focused on the applicability to malicious ICT operations of the notions of self-defense and armed attack under Art 51 UN Charter, of the right to adopt peaceful countermeasures and of the principles of international humanitarian law, as well as at the absence of any mention in the report of the purported need to adopt an international legally binding instrument (see F. Delerue, *The Codification of the International Law Applicable to Cyber Operations: A Matter for the ILC?*, in *ESIL Reflections*, Volume 7, Issue 4, 3 July 2018, available here: esil-sedi.eu/esil-reflection-the-codification-of-the-international-law-applicable-to-cyber-operations-a-matter-for-the-ilc/).

Subsequently, neither the 2021 GGE or OEWG reports showed significant progress in this respect. Both reports did mention the applicability of international humanitarian law and of the principles of humanity, necessity, proportionality and distinction, as well as of the "inherent right of States to take measures consistent with international law and as recognized in the Charter", while clarifying on the one hand that "recalling these principles by no means legitimizes or encourages conflict" (2021 GGE Report, A/76/135, para. 71(f)), and on the other that "discussions on the applicability of international humanitarian law to the use of ICTs by States needed to be approached with prudence" (*Chair's Summary of the 2021 OEWG Report*, A/75/816, Annex II, para. 18).

In turn, the *Draft Final Report* restates, firstly, the applicability of the principles of State sovereignty, equality, non-intervention, peaceful settlement of international disputes, of the prohibition on the use of force, and makes a mere indirect mention to the principles of international humanitarian law as contained in the above quoted 2021 GGE Report. Secondly, the Report adds two important clarifications as to the prohibition on the use of force (*Draft Final Report*, para. 40(a)-(e)). On the one hand, it states that "[a]n ICT operation may constitute a use of force when its scale and effects are comparable to non-ICT operations rising to the level of a use of force" (ibid., para. 40(d)). On the other, it acknowledges that "conduct using ICTs that does not amount to a violation of the prohibition on the threat or use of force may, depending on the circumstances, be contrary to other principles of international law, such as State sovereignty or the prohibition on intervention in the internal or external affairs of States" (ibid., para. 40(e), but see already *Third Annual Progress Report*, para. 37(e)). As obvious as these two statements may seem, they should not be understated. In so doing, the OEWG has, at least partially, aligned itself with the position expressed by several States – indeed, the majority of those that have expressed their views on the matter – as well regional organizations such as the African Union (AU) or in the European Union (EU) in 2024. This is no accident. The OEWG expressly declares having taken into account and discussing the AU and EU common positions, as well as the

above quoted *Second Report on International Law applicable to Cyberspace* adopted by the Inter-American Juridical Committee (CJI/doc. 671/22 rev.2 corr.1, 21 October 2022) and other documents.

Both the AU (Common African position, paras 38-46) and the EU (Common position of the EU, p. 6, 10) have acknowledged the applicability to the cyber-domain of the prohibition on the use of force and of the inherent right of self-defense, and have endorsed the "scale and effects" test as the applicable standard allowing, in principle, to distinguish minor from the most grave violations of prohibition on the use of force, justifying a reaction in self-defense under Art 51 UN Charter. In this context, however, the scale and effects test has in fact been often invoked, as was in this case by the OEWG in the *Draft Final Report*, also to distinguish between cyber-operations amounting to a prohibited use of force and operations that may instead qualify as breaches of the sovereignty of another State or as prohibited interventions in its internal affairs.

An understandably more nuanced position emerges from the CJI's *Second Report* of 2022. While several States (Brazil, Bolivia, Canada and the United States) agreed with the applicability of the prohibition on the use of force to cyber-operations if its scale and effects are comparable to those of a kinetic attack rising to the level of a use of force (CJI, Doc. 671/22 rev.2 corr.1, p. 16), differences emerged, *inter alia*, as to the possibility of drawing a plain analogy between the two types of operations (e.g. Brazil, ibid.), of considering that cyber-operations alone can amount to a prohibited use of force (e.g. Guyana, ibid., p. 17), or *a fortiori* to an armed attack under Art. 51 UN Charter (e.g. Cuba, ibid., p. 22), and as to the possibility of using only cyber means to react to an armed cyber-attack (e.g. Canada, ibid.).

Even though the 2025 *Draft Final Report* makes no reference to self-defense (a question that was left open also by the *Chair's Summary to 2021 OEWG Report*, para. 18) – and indeed this question does not appear among the (non-exhaustive) list of those open for further consideration by the new permanent mechanism –, the above quoted statements represent significant progress in this sense.

With respect to other outstanding issues, further clarifications can be found in the already mentioned 2021 GGE and OEWG reports, and in the 2024-2025 reports of the current OEWG.

Mostly, but not exclusively, these can be drawn from the sections of these reports dedicated to the development and clarification of the norms on responsible State behavior, which are therefore significant when assessing if consensus has emerged as to whether and how international law applies in cyberspace. Despite being framed in hortatory terms, they are intended as reflecting "the expectations and standards of the international community regarding the behaviour of States in their use of ICTs and allow[ing] the international community to assess the activities of States" (II OEWG, *Third Annual Progress Report*, para. 31(a)). More specifically, they are conceived as compatible with applicable rules of international law, which they seek to complement and clarify without, however, limiting or prohibiting action that is otherwise consistent with them (*OEWG Report 2021*, para. 25). In this sense, as mentioned above, they form part of the "cumulative and evolving framework for responsible State behavior in the use of ICTs", together with all the consensus reports of previous working groups, particularly the 2015 GGE final Report, indicated by the UN General Assembly as constituting the starting point for the work of the Sixth GGE as well as the two OEWGs (II OEWG, *Draft of the Final Report*, para. 5). For this reason, the *Draft Final Report* must be read in combination with previous from the same and other working groups. Indeed, the Report does not list all norms but merely provide further indications on consensus reached among States on a few of them before making

final recommendations on continued discussion and implementation (ibid., paras 34-37).

It should in any case be kept in mind that these voluntary norms are "a non-exhaustive list of proposals with *varying levels of support from States* that may be further elaborated upon and supplemented in future discussions" (para. 34, emphasis added). As stated in the Report, additional norms could continue to be developed and in fact several proposals for possible new norms have been put forward and are still being discussed by States and will likely continue to be discussed under the new permanent mechanism (para. 34(o-q)). To facilitate such continued discussion, the *Draft Final Report* address a request to the UN Secretariat to compile and circulate a non-exhaustive list of such proposals, collating those already annexed to the Chair's Summary of the 2021 OEWG Final Report (A/75/816) and proposals for new norms or for elaborating or implementing existing ones emerged during the current OEWG (*Draft Final Report*, para. 36).

In these admittedly narrow terms, these norms can be taken into account when assessing the success of the working groups experience in securing consensus over a hard-core set of principles and rules of international law applicable in cyberspace.

With respect, e.g., to the law of international responsibility, and particularly the issue of attribution, norms 1.2-1.3, as formulated in UNGA res. 73/27 provide, first, that "States must meet their international obligations regarding internationally wrongful acts attributable to them under international law", that they must not use proxies to commit such acts – which in turn means that they are also responsible for entities owned or controlled by them (Chair's Summary of the I OEWG Report, 2021, A/75/816, para. 14) – and that they have a due diligence obligation not to allow their territory to be used for internationally wrongful acts using ICTs. The latter principle is, in particular, restated in the 2025 *Draft Final Report* with the further clarification that this due diligence obligation "must also be met with respect to non-State actors within a State's territory" (para. 34(c)). This is certainly a truism. However, on the one hand, it certainly underscores that malicious operations are, more often than not, carried out by non-State actors. On the other, while it appeared in the 2021 GGE Report, which noted that "a State should not permit another State or non-State actor to use ICTs within its territory to commit internationally wrongful acts", it was surprisingly absent from the previous report of the current OEWG. It is also certainly in line with analogous and more detailed statements contained in the common positions of the AU (Common African position, paras 18-24) and the EU (Common position of the EU, pp. 5-6, 8), mentioned above, as well as with the indication in the OEWG's 2025 *Draft Final Report* that the topics open for further consideration include, *inter alia*, "the obligations of non-State actors in the use of ICTs" (ibid., para. 41(b)). Further clarifications on how to apply this principle in the cyber-domain were provided by the 2021 GGE Report, mentioning the requirements of proportionality, appropriateness, effectiveness and compliance with international and domestic law in a State's monitoring of ICT activities, as well as cooperation with other States and the private sector in addressing internationally wrongful acts originating from its territory or ICT infrastructure, and procedural steps to implement such cooperation (such as notification of cyber incidents to the origin State) (A/76/135, para. 30). Second, the above quoted norms caution against misattributions by providing, on the one hand, that the mere indication that an ICT activity was launched or otherwise originates from the territory or the ICT infrastructure of a State may be insufficient in itself to attribute the activity to that State. Third, they lay down elements that should be taken into account in the attribution of ICT activities, recommending the consideration "of 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" (A/73/27, norm 1.2; see also the factors listed in the 2021 GGE Report, para. 24).

While the law of State responsibility does not contain a generally applicable evidentiary standard, the principles and criteria contained in these norms appear to be in line with the notion that attribution of a certain conduct to a State is possible under the rules laid down in the International Law Commission's Articles on the responsibility of States for internationally wrongful acts (ARSIWA, 2001, Arts. 4-11). This has been, in fact, confirmed by several States in their national position papers (see, for a comprehensive account, the International Cyber Law Interactive Toolkit prepared by the The NATO Cooperative Cyber Defence Centre of Excellence, available at: cyberlaw.ccdcoe.org/wiki/Main_Page) and, again, by the common positions of the AU (Common African position, para. 61) and of the EU (Common position of the EU, p. 8).

One further aspect that deserves consideration is the notion of critical infrastructure (CI) and their protection. Norms 1.6 to 1.8 in UNGA res. 73/27 (norms (f) to (h) in the 2021 GGE Report, A/76/135, paras 42-55) lay down a duty not to "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", as well as to protect their CI taking into account UNGA res. 58/99 of 30 January 2004 on the *Creation of a global culture of cybersecurity and the protection of critical information infrastructures*, and to respond to requests for assistance or mitigation of harmful ICT activities originating from their territory against CI of another State. The *Draft Final Report* reiterates in this respect that attacks against CI or Critical Information Infrastructure (CIIs) pose "an elevated risk of harm to the population and can be escalatory" (para. 34(d)) and emphasizes the need for cooperation – suggesting the development of common templates for requesting and responding to requests for assistance, but also the sharing of best practices, national policies, –, and protection, confirming in this respect that each State is solely responsible for determining which infrastructures it designates as critical, as was already recognized in UNGA res. 58/99. In this sense, neither the current and past OEWG, nor the GGEs have attempted to devise a commonly accepted definition of CIs. More indications can in any case be found in the 2021 GGE and OEWG reports, pointing out that such infrastructures "form the backbone of a society's vital functions, services and activities" and that "if these were to be significantly impaired or damaged, the human costs as well as the impact on a State's economy, development, political and social functioning and national security could be substantial" (*2021 GGE Report*, A/76/135, para. 43). Nonetheless, States retain complete freedom in the designation, which has allowed some States, e.g. the United States, to expand the notion at the point of including, e.g. commercial facilities such as the Las Vegas casinos or motion picture studios (see D. Riedman, *Questioning the Criticality of Critical Infrastructure: A Case Study Analysis*, in *Homeland Security Affairs* 12, Essay 3, May 2016, available here: www.hsaj.org/articles/10578), which have been the target of cyber-attacks (see K. Eichensehr, *Cybersecurity, Elections, and Critical Infrastructure at Home and Abroad*, in *Just Security*, 4 August 2016, available here www.justsecurity.org/32276/cybersecurity-elections-critical-infrastructure-home/).

Finally, the Report encourages States to continue exchanging views and engaging in focused discussion both in the new permanent mechanism and through the adoption and sharing of national positions on how international law applies in cyberspace. To facilitate continued discussion a request is made to the UN Secretariat to compile and circulate a non-exhaustive list of proposals of new norms of responsible State behavior, collating those already annexed to the Chair's

Summary of the 2021 OEWG Final Report and those emerged during the current OEWG (*Draft Final Report*, para. 36).

Ultimately, the *Draft Final Report* appears to take a few, although arguably still minor steps towards a consensus on how international law applies in cyberspace, especially in some of the most contentious areas that had prevented agreement in the past. It is, in any case, on cooperation, confidence- and capacity-building measures, as well as implementation of existing voluntary norms that the Report's emphasis is placed.

3. – In fact, much of the *Draft Final Report* is dedicated to confidence- and capacity-building measures, as well as to the implementation of the above discussed norms of responsible State behavior in cyberspace, with the adoption of a *Voluntary Checklist of Practical Actions for the implementation of voluntary, non-binding norms of responsible State behaviour in the use of ICTs* (Draft Final Report, Annex I), which are recommended for adoption by States (*Draft Final Report*, para. 37). Indeed, several norms are devoted to confidence- (norms 1.9-1.11, and 1.13 of UNGA res. 73/27 on supply-chain integrity, prevention of malicious ICT use, reporting of vulnerabilities and sharing of information, and involvement of the private sector and civil society in improving security of ICTs and supply chain) and capacity-building (norm 1.12 on protection of authorized emergency response teams, whose establishment has been repeatedly recommended by the current OEWG and previous working groups; but see also the recommendation to States in a position to do so to continue capacity-building efforts in areas of international law, at paras 41(d) and 44) as well as to implementation (norms 1.13 on the involvement of the private sector and civil society on implementation of norms of responsible State behavior).

More generally, however, the Report encourages support for, and effective implementation of several initiatives already launched by the current OEWG. To name but a few, with regard to confidence-building measures, the Report notes the continued support for the Global Points of Contact (POC) Directory launched on 9 May 2024 and expresses appreciation for the continued six-monthly "ping" test of the Global POC Directory initiated by the UN Secretariat (Draft Final Report, para. 45(b)). It calls for the continued expansion and operationalization of the Global POC Directory, by calling on States that have not yet done so to nominate national POCs and to adopt the "Template for Communication" between POCs developed by the UN Secretariat (ibid., paras 45(c) and 49), and encourages implementation of the "Initial List of Voluntary Global Confidence-Building Measures" contained in Annex B of the *Third Annual Progress Report* of July 2024 (ibid., para. 45(h)).

The Report further recalls and reaffirms the capacity-building principles adopted by the 2021 OEWG Report (A/75/816, para. 56 and contained in the current OEWG's *Second Annual Progress Report*, 28 July 2023, UN Doc. A/AC.292/2023/CRP.1, Annex C), and the need for their mainstreaming. It further welcomes the UN Secretariat's proposal and recommends the establishment of the Global Information and Communication Technologies Security Cooperation and Capacity Building Portal (GSCCP, UN Doc. A/AC.292/2025/1), which could serve both as: "(a) the official website of the future permanent mechanism; (b) a central location for providing practical information on ICT security events to foster the active participation of States; and (c) a platform to facilitate the sharing of information relating to best practices and capacity-building", by harmonizing it with resources from existing and related online portals (*Draft Final Report*, para. 51(e-f)).

Finally, with regard to the implementation of norms of responsible State behavior, the Draft Final Report includes in Annex I a detailed, but non-exhaustive

set of Practical Actions in the form of a "Voluntary Checklist". These are intended as "a voluntary capacity-building tool" that could serve as a starting point to support States' implementation efforts. The envisaged actions can be at the national or international level and they include, e.g., the establishment of Computer emergency/security incident response teams (so-called CERTs or CSIRTs), and accompanying national coordination structures and mechanisms, or more generally the participation in international or regional processes related to ICT security, the exchange of information, best practices and lessons learned, and the request and offer of assistance related to ICT incidents.

4. – As mentioned in the introduction, the current OEWG will soon conclude its work and a new, permanent mechanism will be established pursuant to the proposal prepared by the OEWG and contained in Annex C of the *Third Annual Report* of July 2024 (A/79/214), which was endorsed by the General Assembly in resolution 79/237.

The establishment of a future mechanism for "regular institutional dialogue" under the auspices of the United Nations already appeared in the mandate of the First OEWG under UNGA res. 73/27. The 2021 OEWG Report concluded that any such mechanism "should be an action-oriented process with specific objectives, building on previous outcomes, and be inclusive, transparent, consensus driven, and results-based (A/75/816, para. 74).

In its proposal, the current OEWG devised an open-ended and action-oriented mechanism which will adopt as the basis for its work the take as the foundation of its work "the consensus agreements on the framework of responsible State behaviour in the use of ICTs from previous OEWG and GGE reports with the aim of continuing to promote an open, secure, stable, accessible, peaceful and interoperable ICT environment" and an "open, inclusive transparent, sustainable and flexible process which would be able to evolve in accordance with States' needs and as well as in accordance with developments in the ICT environment" (A/79/214, Annex C, para. 1 and 4(b-c)).

The future "Open-Ended Action-Oriented Permanent Mechanism on ICT Security in the context of international security" will be permanent in character (unlike previous working groups) State-led – i.e. negotiations and decisions on ICT security will remain the prerogative of States –, and single-track, to avoid the duplication seen between 2019 and 2021.

Like the OEWGs, it will be open to all members and will allow contributions from other interested actors, such as the private sector, non-governmental organizations having consultative status before the Economic and Social Council pursuant to resolution 1996/31, and academia (ibid., paras 6 and 11), arguably including the International Law Commission, as also emphasized by the OEWG's Draft Final Report with respect to the recommendations concerning continued discussion on international law (Draft Final Report, para. 41(a)), as well as on confidence- and capacity-building measures (ibid., paras 45(j) and 51(m)). In addition, the Draft Final Report has also laid down a set of "Additional Elements on Modalities on the Participation of Other Interested Parties and Stakeholders, including Businesses, Non-Governmental Organizations and Academia" (ibid., Annex III), which cover accreditation, rights of participation (which remain strictly consultative and technical in nature).

The new permanent mechanism will be entrusted with several functions that have been so far carried out by the OEWGs. Building upon the outcomes of the Open-ended Working Group 2021-2025 and previous OEWG and GGE, the new permanent mechanism will strengthen the ICT security capacity of all States, including by developing further and assisting in the implementation of the cumulative and evolving framework for responsible State behavior in the use of

ICTs. It will address issues such as, *inter alia*, existing and potential threats; voluntary, non-binding norms of responsible State behavior, the ways for their implementation and the development of additional norms; how international law applies in the use of ICTs, considering the possibility of future elaboration of additional binding obligations, if appropriate; and finally the development and implementation of confidence-building and capacity-building measures.

The mechanism will be set up as a subsidiary organ of the General Assembly reporting to the First Committee and, as the previous OEWGs and GGes, it will benefit from the secretarial services of the UN Office for Disarmament Affairs. It will take all its decisions based on the principle of consensus.

As mentioned above, the GSCCP will likely function as a dedicated website of the mechanism, while the Global POC Directory will serve as a voluntary standing tool for use by States. It will function in a five-year cycle consisting of two biennial cycles followed by a one-year review cycle and will convene in annual Substantive Plenary Sessions, whose work will be organized in accordance with the pillars of the framework for responsible State behavior in the use of ICTs (Draft Final Report, Annex III, Additional Elements on Structure, including Dedicated Thematic Groups, para. 5).

Dedicated Thematic Groups will aim to build on and complement the discussions in the substantive plenary sessions. They will provide the opportunity for more detailed and action-oriented discussions, allowing in particular the participation of experts. Following the recommendation of the General Assembly in res. 79/237, the Draft Final Report has proposed the establishment at the first session of the new permanent mechanism (scheduled for March 2026) of three thematic groups: one dedicated tasked with considering action-oriented measures to "increase the resilience and ICT security of States", including the protection of CI, "enhance concrete actions and cooperative measures to address ICT threats and to promote an open, secure, stable, accessible and peaceful ICT environment", and promote "maintaining peace, security and stability in the ICT environment" (ibid., para. 8); one dedicated to "continue discussions on how international law applies to the use of ICTs in the context of international security"; and finally one dedicated to capacity-building.

Additionally, the Chair will be able to convene, as necessary, Dedicated Intersessional Meetings to engage in additional discussions on specific issues, in consultation with States. At the end of each five-year cycle, a Review Conference will be convened "to review the effective functioning of the future permanent mechanism and provide strategic direction and guidance" for the subsequent cycle.

5. – The anticipated conclusion of the work of the current OEWG carries with it the question of how effective the working groups negotiation format has been in securing consensus in the several areas under its purview. With regard to the fundamental problem of whether and how international law applies to States' ICT activities, a mere comparison with the common positions of several regional organizations mentioned above cannot but lead to the conclusion that this twenty-year process, despite the minor progress outlined above, has not been very effective. The strikingly low level of clarity and detail on the several principles and rules of international law, and even of the voluntary, non-binding norms of responsible State-behavior, demonstrates, rather than the persistent differences among States, the fact that this question appears to have fallen behind in the list of priorities of the most recent working groups. Despite the statement contained in the proposal concerning the future permanent mechanism that regional and sub-regional organizations' work on ICT security, while important, is to be understood as complementary to, and has to be integrated with that of UN-based organisms, it is clear that there is a risk of fragmentation of the relevant regulatory framework.

DPCE online
ISSN: 2037-6677

It remains to be seen whether the future permanent mechanism will be able to make significant progress in this respect. As it has recently been noted by a leading scholar, the consistent confirmation of the need to establish such a common framework "is not sufficient to give the negotiation process the necessary impetus to achieve concrete results within a reasonable period of time. Especially in the current international context in which confrontation and hegemonic aims prevail over dialogue (P. Gargiulo, *The United Nations and Cybersecurity*, cit., p. 216).

Andrea Insolia
Dipartimento Diritto e Istituzioni
Universitas Mercatorum, Roma
andrea.insolia@unimercatorum.it