RESEARCH IN FOCUS

Reflections on the Pre-draft of the report of the OEWG on developments in the field of ICTs in the context of international security

François Delerue
Xymena Kurowska
Patryk Pawlak

April 2020

EU CYBER DIRECT
Supporting EU Cyber Diplomacy

This project is funded by the European Union.

About the authors

Dr François Delerue is a researcher in cyber defence and international law at the Institute for Strategic Studies, French Military School (IRSEM).

Dr Xymena Kurowska is Associate Professor at Central European University (CEU) in Budapest and Vienna.

Dr Patryk Pawlak is the EUISS Brussels Executive Officer and Project Coordinator for the EU Cyber Direct.

Contents

Introduction 2

1. Existing and potential threats 2

2. International law 2

3. Rules, norms and principles 3

4. Confidence-building measures 4

5. Capacity building 5

6. Regular institutional dialogue 5

7. Final observations 6

8. Summary of the proposals 7

Introduction

The United Nation is increasingly focused on fast-developing issues in the field of information and telecommunications in the context of international security. This increased focus provides a useful opportunity for taking concrete actions that strengthen the commitment of states to responsible behaviour in cyberspace. The Pre-draft of the report of the OEWG, presented by its Chair, provides a welcome opportunity for the international community – not only states but also civil society, the technical community, and the private sector – to make concrete suggestions and recommendations to this effect. Building on observations made earlier during the EU-UNGGE consultation with civil society conducted in 2019, we would like to encourage the Chair to ensure that the months of efforts and discussions, in the context of the OEWG, translate into an ambitious final report that commits the international community to fostering a resilient digital society with full respect for human rights and the rules-based order.[1] In this spirit, we would like to offer some preliminary observations on the content of the Pre-draft.

1. Existing and potential threats

We welcome a broad view adopted in the Pre-draft as to the nature of the threats faced by our societies in the digital domain. We agree that the interconnected nature of our increasingly digitalized societies poses new risks and creates new vulnerabilities. However, we think that certain parts of this section require more nuanced language. In particular, the suggestion that 'a lack of awareness, resilience and adequate capacities constitutes a threat in and of itself' might unfairly stigmatise and alienate states with limited resources. While we agree that all states should aim to strengthen their resilience and cyber capacities, we think that equalizing threats to our societies resulting from malicious activities by state and non-state actors with their limited capacities is unjustified, especially given that the current evidence demonstrates that most malicious activities originate from states with well-developed cyber capabilities. **Instead, we recommend that the report further stresses the need to address the lack of awareness, resilience, and adequate capacities as a priority for cyber capacity building initiatives.**

2. International law

The Pre-draft report continues to raise general questions about the application of existing international law in cyberspace rather than addressing specific points on the application of specific rules and principles of international law. Further reflection on the latter aspect might prove particularly useful.

2.1 Sources and bodies of international law: Paragraph 24 discusses the bodies of international law. We believe there is a confusion in this paragraph between sources (customary international law) and branches of international law (international humanitarian law, international human rights law, international criminal law). Article 38 of the Statute of the International Court of Justice, annexed to the Charter of the United Nations, recalls the sources of international law, including treaty law and customary international law. **We believe that the report and the discussion would gain in clarity if it contained two different paragraphs, one dedicated to the sources of international law and one on the branches of international law.**

[1] Patryk Pawlak, Xymena Kurowska, Eneken Tikk, Caitriona Heinl, François Delerue (2019) Pathways to Change: Resilience, Rights and Rules in Cyberspace, Input paper for the EU-UNGGE regional consultations, June 2019. Available at: https://eucyberdirect.eu/wp-content/uploads/2019/06/pawlak-kurowska-tikk-heinl-delerue-1.pdf

2.2 New legal instrument: Regarding the need for a new legal instrument, we would like to recall the skepticism towards this idea, and the debate surrounding the application of international law to cyber operations, that was expressed during the intersessional meeting in December 2019.[2] Questions on the applicability of international law, and on the application of the rules and principles of international law, may be seen as two sides of the same coin. However, the delineation of the relevant rules and principles of international law is not so straightforward. Indeed, it leads to another question: which rules and principles of international law should be applied and what is their content and limits. Conversely to domestic law, the vast majority of the rules and principles of international law are vague, offering to the subjects of international law a high degree of flexibility and adaptability in the interpretation and application of these rules and principles. **Building on these observations, the central question regarding the delineation of the rules and principles of international law applicable to cyber operations is the determination of how to distinguish between what States need to agree upon and what should be left for the unilateral interpretation of each State.** The prohibition of the use of force in article 2, paragraph 4, of the Charter of the United Nations offers a good illustration. This prohibition is written in very general terms and does not include any definition of what constitutes 'force'. No subsequent legal instrument has been adopted to clarify the definition of force in general, nor in a specific context. The interpretation of what constitutes force has been developed through unilateral declarations made by States, State practice, political discussions and rulings of the International Court of Justice. Thus, why would it be different regarding the use of force in cyberspace?

2.3 International humanitarian law: The draft report would also benefit from more clarity regarding the applicability of international humanitarian law. International humanitarian law (IHL) is applicable during an armed conflict, either of international or non-international character. Thus, international humanitarian law is not applicable to the vast majority of cyber operations, since they take place outside of an any armed conflict. However, certain cyber operations are perpetrated within armed conflicts. In such cases, the applicability of international humanitarian law is indisputable. **We believe that one of the reasons for the debate surrounding IHL might result from the lack of sufficient distinction and clarity about the applicability of IHL and concrete application of its principles. Therefore, we suggest that the report better reflects these two different questions.**

3. Rules, norms and principles

The UN-led processes have devoted significant attention to the question of norms of responsible behaviour in cyberspace. In recent years, several multistakeholder initiatives have contributed to this discussion by proposing new norms. Without engaging in the debate regarding whether such norm entrepreneurship is desirable and how these new norms have proliferated in the international discourse, the following points deserve additional attention during further reflection.

3.1 Linkages between norms and international law: Some of the norms adopted in the UNGGE reports and Resolution establishing OEWG are rooted in the existing rules and principles of international law; others provide additional guidance on how to interpret the existing internationally legally binding obligations. These norms, however, do not make any explicit reference to the rules or principles of international law from which they have been derived. In the 2015 Report of the UNGGE (A/70/174), for instance, norm 13(c) stipulates that: "States should not knowingly allow their territory to be used for internationally wrongful acts using ICTs". It is a clear interpretation of the principle of due diligence into the cyber realm. Yet, the norm makes no reference to this principle

[2] François Delerue, 'International law in cyberspace: Are we asking the right questions?', Paper based on the statement delivered at the Informal intersessional consultative meeting of the OEWG with industry, non-governmental organizations and academia (2-4 December 2019), EU Cyber Direct. Available at: https://eucyberdirect.eu/content_events/intersessional-multistakeholder-meeting-at-the-oewg/

(which is also refered to in the section of the Report dedicated to international law, i.e. para. 28e). This poses two sets of problems: a) it creates confusion between rules and principles of international law and non-binding norms; b) the interpretative norm and the obligation of international law on which it is built might evolve in two different direction, creating a risk of incoherence challenging the international-rules based order. **Therefore, the current draft might benefit from a clearer distinction between two types of norms of responsible behaviour: a) norms interpreting or providing guidance on existing rules or principles of international law. These norms should explicitly refer to their international legal sources and be bound by these sources in their future evolution; b) norms of responsible behaviour without any clear link with international law.** Such a distinction will bring clarity in the work of the OEWG and could potentially contribute to the work in the UN Group of Governmental Experts. Moreover, it would help identifying and distinguishing the role of each type of norms in the interpretation and progressive development of international law.

3.2 Operationalisation of norms: In connection with paragraph 38 which states the importance of leaving to states how they operationalise cyber norms, we would like to underscore that the very term 'operationalisation' implies that there is a consensus on the meaning of cyber norms. While there is an agreement on the general purpose of cyber norms – and that many of them can indeed be traced in regulatory and institutional arrangements adopted at national and regional levels - the current practice demonstrates that state and non-state actors diverge on how they understand specific norm prescriptions (i.e. what is considered responsible behaviour) and on norm parameters (in which situation these norm prescriptions apply).[3] **The most promising path towards a robust global normative framework is therefore through the exchange of good practices as well as a greater integration of the input by regional organisations and their interpretations of cyber norms with a global multilateral framework**. Highlighting the interlinkage between norms and CMBs as stated in paragraph 34, we would like to emphasise that **CBMs can become a platform for a greater consideration of regional understandings of global cyber norm, and thus can become a mechanism for a better adjustment and specification of the global normative framework, in line with the principle of local ownership.**

4. Confidence-building measures

The Pre-draft rightly stresses the importance of confidence-building measures in preventing conflicts by addressing misperceptions and misunderstandings and reducing the risk of escalation. The call for concrete actions in the implementation of confidence-building measures at the global level deserves particular attention. In this regard, current experiences with CBMs demonstrate the key role of the regional and sub-regional organisations in preparing the ground and creating favourable conditions for the development and implementation of CBMs. Therefore, we support the idea of further encouraging the exchange of good practices and lessons from the regional initiatives at the global level, without duplicating any existing efforts, in order to identify success stories and possible gaps that might need to be addressed at the global level. **We are of the view that, in the current political context, supporting regional and inter-regional cooperation on CBMs, with closer cooperation at the global level when appropriate, offers the most promising avenue for advancing the practical implementation of CBMs.**

[3] Xymena Kurowska, "The politics of cyber norms: Beyond norm construction towards strategic narrative contestation", Research in Focus, March 2019. Available at: https://eucyberdirect.eu/content_research/the-politics-of-cyber-norms-beyond-norm-construction-towards-strategic-narrative-contestation/

5. Capacity building

The preamble of the Resolution 73/27 establishing the Open-ended Working Group notes the importance of capacity-building as an essential element for cooperation of states, confidence-building and promoting the use of ICTs for peaceful purposes. We welcome the fact that the foundational role of cyber capacity building as a cross-cutting issue is acknowledged throughout the document

5.1 Principles for cyber capacity building: Building on decades of experience with capacity building, **we would like to support the call for a principled approach to strengthening cyber capacities globally**. Such principles can be derived from the Busan Partnership, the Delhi Communiqué as well as the Council Conclusions on the External Cyber Capacity Building Guidelines[4] adopted by the European Union and the Operational Guidance for the EU's International Cooperation on Cyber Capacity Building.[5]

5.2 Coordination of efforts: The Pre-draft suggests that the existing platforms within the UN and in the global community could be used to strengthen coordination on cyber capacity building. Topics to be covered through such coordination include sharing national views on capacity-building requirements, encouraging the sharing of lessons and experiences from both recipients and providers of support, and facilitating access to information on capacity-building and technical assistance programmes. **We believe that, while these goals are critical for effective and sustainable cyber capacity building, they might be better achieved through cooperation within the existing regional organisations and bodies, in particular the Global Forum on Cyber Expertise.** Given the importance of cyber capacity building for the debate about design and implementation of norms, confidence-building measures, international law and societal resilience, **we propose that the OEWG report put forward the list of concrete "Cyber Capacity Goals" (CCGs) to be achieved by the international community by 2030.** The starting point for such a list could be the 2015 report of the UN Group of Governmental Experts and other elements identified by the cyber capacity building community (e.g. adopting a national cyber security framework, establishing a CERT, etc.). Consequently, the UN could champion the global agenda based on such CCGs and provide a much-needed political support for the cyber capacity building.

6. Regular institutional dialogue

The continued engagement of civil society, the technical community, and the private sector along with governments in the discussions on the use of ICTs in the context of international security – including under the umbrella of the OEWG – underlines the relevance of this topic for the whole international community. Therefore, we **support the idea that any future dialogue under the UN umbrella should build on previous agreements, be inclusive, consensus- and evidence-driven, result-oriented, and sustainable.** We believe that such a dialogue needs also to reflect the diversity of views and interests represented by different communities. Therefore, we ask the Chair to further reflect on the need for additional institutionalization of the ongoing debates through a politically binding instrument or inter-governmental specialized agency. Instead, **we suggest that a regular institutional dialogue is pursued by establishing concrete cooperation mechanisms with regional organisations and specialized bodies that regularly engage in shaping policies in the cyber domain.** Such an approach would also ensure stronger ownership of the specific solutions that might originate through discussions at the global level.

[4] http://data.consilium.europa.eu/doc/document/ST-10496-2018-INIT/en/pdf

[5] https://op.europa.eu/en/publication-detail/-/publication/508a8d73-a426-11e8-99ee-01aa75ed71a1/language-en/format-PDF/source-117729241 and https://op.europa.eu/en/publication-detail/-/publication/a90640f1-a423-11e8-99ee-01aa75ed71a1/language-en

6.1 New open-ended working group and group of governmental experts: While we believe that both these venues have significantly contributed to making the discussion about responsible state behaviour in cyberspace more inclusive and transparent, we do believe that such work should continue on the basis of clearly identified gaps, policy challenges and questions that require further discussion. In that sense, **the OEWG report should clearly indicate areas of agreement – but also disagreement – that would provide guidance for possible discussions in the future.**

6.2 Sponsorship programmes and support mechanisms: The experience of the current OEWG clearly demonstrated the need for significant resources required to facilitate the participation of the broader stakeholder community, especially from the Global South. The intersessional meeting in December shows the value of such broad engagement – both in terms of ensuring greater transparency and including new and underrepresented perspectives.[6] Given the significant effort and resources committed by states and organisations engaged in establishing such sponsorship and support mechanisms as well as the long-term commitment by those benefiting from such mechanisms, we believe that **the final OEWG report should better reflect the spirit and the content of the debates, in particular by going beyond state-centric wording of the current report.**

7. Final observations

While recognising that the final report of the OEWG needs to be concluded by consensus, we believe it is important for the final report to be as ambitious as possible. A similar expectation was expressed by numerous civil society organisations and the private sector during the inter-sessional meeting organized in December 2019, as captured in the informal conclusions drafted by Mr David Koh, Chair of the intersessional multi-stakeholder meeting (2-4 December 2019). Unfortunately, many ideas presented at that meeting have not been included in the Pre-draft. Although point 7 of the Pre-draft states that "the OEWG has benefited from exchanges with representatives from inter-governmental organizations, regional organizations, non-governmental organizations, the private sector and academia", the current version of the document does not reflect that spirit**. Therefore, we recommend that the revised draft report better reflects the depth of contributions made by other stakeholders (business, non-governmental organizations, and academia). In addition, we suggest that the informal conclusions drafted by Mr David Koh be annexed to the OEWG final report.**

The recommendations proposed in the Pre-draft seem to suggest an increased role for the United Nations in supporting exchange of good practices, lessons, and improving coordination in various policy areas. However, any such potential decisions should take into account potential risks that they entail:

7.1 Feasibility and limited resources: several of the recommendations (e.g. creation of multiple global repositories) entail committing significant resources for their implementation. We suggest further assessment of their feasibility, including the identification of mechanisms and tools through which the UN could support the implementation of these recommendations.

7.2 Hollowing out existing initiatives: some of the recommendations suggest increased involvement of the UN (e.g. on cyber capacity building). While we recognize the importance of international cooperation and multilateral approaches in addressing many of the challenges identified in the Pre-draft, we recommend a more nuanced approach that does not undermine the existing efforts and initiatives, in particular those undertaken by the regional organisations and bodies.

[6] The EU Cyber Direct – through the EU Engagement Support Mechanism – facilitated participation of 39 participants out of whom 27 made interventions during the intersessional meeting.

8. Summary of the proposals

a) The report should stress the need to address the lack of awareness, resilience, and adequate capacities as a priority for cyber capacity building initiatives.

b) The central question regarding the delineation of the rules and principles of international law applicable to cyber operations is the determination of how to distinguish between what States need to agree upon and what should be left for the unilateral interpretation of each State. We believe that one of the reasons for the debate surrounding IHL might result from the lack of sufficient distinction and clarity about the applicability of IHL and concrete application of its principles. Therefore, we suggest that the report better reflects these two different questions.

c) The current draft might benefit from a clearer distinction between two types of norms of responsible behaviour: 1) norms interpreating existing rules and principles of international law and 2) norms of responsible behaviour that are not linked to any international legal obligations. The first categoy of norms should explicitly refer to their international legal sources and be bound by these sources in their future evolution

d) CBMs can become a platform for a greater consideration of regional understandings of global cyber norm, and thus can become a mechanism for a better adjustment and specification of the global normative framework, in line with the principle of local ownership.

e) We are of the view that, in the current political context, supporting regional and inter-regional cooperation on CBMs, with closer cooperation at the global level when appropriate, offers the most promising avenue for advancing the practical implementation of the CBMs.

f) We believe that many of the objectives mentioned in the cyber capacity building section are critical for resilient societies. Therefore, international cooperation of such efforts is essential. However, we believe that this function might be better achieved through cooperation within the existing regional organisations and bodies, in particular the Global Forum on Cyber Expertise.

g) We propose that the OEWG report put forward the list of concrete "Cyber Capacity Goals" (CCGs) to be achieved by the international community by 2030.

h) We support the idea that any future dialogue under the UN umbrella should build on previous agreements, be inclusive, consensus- and evidence-driven, result-oriented, and sustainable. We suggest that a regular institutional dialogue is pursued by establishing concrete cooperation mechanisms with regional organisations and specialized bodies that regularly engage in shaping policies in the cyber domain.

i) The revised draft report should better reflect the depth of contributions made by other stakeholders (business, non-governmental organizations, and academia) throughout the process. In addition, we suggest that the informal conclusions drafted by Mr David Koh be annexed to the OEWG final report.

About EU CyberDirect

The **EU Cyber Direct** project supports EU cyber diplomacy efforts and consequently contributes to the development of a secure, stable and rules-based international order in cyberspace through extensive dialogues with strategic partner countries and regional/international organisations. The **EU Cyber Direct** is funded by the European Commission under the Partnership Instrument, International Digital Cooperation project: Trust and Security in Cyberspace.

RESEARCH IN FOCUS

is a series of research papers aimed at supporting the EU's cyber-related policies by providing a timely and policy-relevant analysis.

EU CYBER DIRECT

This project is funded by the European Union.