ESIL Reflections
Editorial Board: Samantha Besson, Jean d'Aspremont (Editor-in-Chief), Jan Klabbers and Christian Tams

3 July 2018 Volume 7, Issue 4

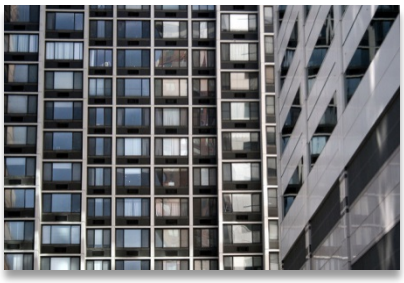

Image by polkadot (cc)

The Codification of the International Law Applicable to Cyber Operations: A Matter for the ILC?

François Delerue *

Institut de Recherche stratégique de l'École Militaire

The failure to reach a consensus on a final report of the United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (UNGGE) in June 2017 questions the future of the multilateral discussions on cybersecurity and cyberdefense, and more specifically the application of norms of international law to cyber phenomena.

In this context, this Reflection advocates that States should consider to dissociate the discussions regarding the applicability and application of norms of international law from the political and strategic discussions, including those on norms of behaviour and confidence-building measures. Such political and strategic discussions, it is argued, should remain an interstate diplomacy exercise, while discussions on the legal framework should be referred to an international body comprised of legal experts rather than diplomats and State representatives, namely the International Law Commission (ILC) of the United Nations.

It is worth noting that the applicability of international law, and the UN Charter, had been recognized in the consensual reports of the two previous UNGGE in 2013 (UN Doc A/68/98, para 19) and 2015 (UN Doc A/70/174, para 24). Several States confirmed this position in their comments on these reports[1] and in their national cyberdefense and cybersecurity strategies.[2]

* François Delerue is a research fellow in cyber defense and international law at the Institute for Strategic Research (IRSEM – Institut de Recherche stratégique de l'École Militaire), an associate researcher at the Castex Chair of Cyber Strategy and an adjunct lecturer at Sciences Po Paris. He completed his Ph.D.

Similarly, the general applicability of international law to cyber operations is generally not contested in the literature. Thus, the question is not whether international law is applicable to cyber operations but to determine how norms of international law apply to cyber operations.

It is worth pointing out that referring the codification of cyber international law to the ILC would neither constitute a panacea nor end hostile cyber activities by States and their proxies. We should not be naive on that point. Nevertheless, referring the matter to the ILC would have some advantages over existing fora or previous endeavours. From this perspective, this Reflection compares the potential of referring to the ILC with the UNGGE and the *Tallinn Manual Process*, which led to the adoption of the two editions of the *Tallinn Manual on the International Law Applicable to Cyber Operations* published in 2013 and 2017.[3] The two editions of the *Tallinn Manual* were drafted by a group of experts, headed by Professor Michael N. Schmitt and given material support of the NATO Cooperative Cyber Defence Centre of Excellence (CCDCoE) but do not represent the view of the NATO CCDCoE, NATO or its Member States. They constitute to date the most comprehensive academic publication on the subject. The objective of this Reflection is not to criticize the UNGGE or the *Tallinn Manual*, or any similar initiative, but to use them as a basis for the discussion on the ILC, mainly because they constitute the two most advanced processes on the interpretation of cyber international law. Both the *Tallinn Manual* process and, to a certain extent, the UNGGE aimed at answering the question on how norms of international law apply to cyber operations and to codify them. For these reasons, I believe they offer appropriate examples that can be compared to the proposal to refer the matter to the ILC.

---

on cyber operations and international law at the European University Institute (EUI – Florence, Italy) in November 2016, under the supervision of Professor Nehal Bhuta. francois.delerue@eui.eu

[1] See notably: UNGA 'Report of the Secretary-General on Developments in the Field of Information and Telecommunications in the Context of International Security (Addendum)' (9 September 2013) UN Doc A/68/156/Add.1; UNGA 'Report of the Secretary-General on Developments in the Field of Information and Telecommunications in the Context of International Security' (30 June 2014) UN Doc A/69/112; UNGA 'Report of the Secretary-General on Developments in the Field of Information and Telecommunications in the Context of International Security (Addendum)' (18 September 2014) UN Doc A/69/112/Add.1.

[2] See for instance: France, R*evue stratégique de cyberdéfense* (February 2018), 82, 85 and 87, http://www.sgdsn.gouv.fr/evenement/revue-strategique-de-cyberdefense/; Australia, *Australia's Cyber Security Strategy: Enabling Innovation, Growth & Prosperity* (April 2016) 7, 28, 40-41, https://cybersecuritystrategy.pmc.gov.au/assets/img/PMC-Cyber-Strategy.pdf; Russian Federation, *Doctrine of Information Security of the Russian Federation* (December 2016), §34, http://www.mid.ru/en/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/2563163; United-Kingdom, National Cyber Security Strategy (November 2016), 63, https://www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021.

[3] Michael N Schmitt (ed), *The Tallinn Manual on the International Law Applicable to Cyber Warfare* (Cambridge University Press 2013); Michael N Schmitt and Liis Vihul (eds), *The Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (2nd edn, Cambridge University Press 2017).

A short preliminary remark is necessary. The following argument may be construed as a manifestation of the so-called the 'interventionist and managerial project' informing the international legal scholarship that is currently grappling with cyber operations.[4] In this respect, it worth emphasizing that the objective of this Reflection is not to determine or decide whether norms of international law apply and how they should be interpreted, but rather to discuss a possible forum to restart and continue discussions that have failed so far. This Reflection focuses on the format, and not the content, of these discussions. Yet, this Reflection is premised on the assumption that international law regulates state-sponsored cyber operations and offers, to some extent, an effective framework to govern State cyber activities.

1. The Success and Failure of the UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (UNGGE)

The developments in the field of information and telecommunications in the context of international security have been discussed by the UN General Assembly since 1998 and resulted in the adoption of the Resolution 53/70 on 4 January 1999. Since then, the UN General Assembly has adopted several resolutions on the matter.

One of the main achievements of these resolutions is the establishment of five successive UNGGEs on the Developments in the Field of Information and Telecommunications in the Context of International Security in 2004, 2009, 2012, 2014 and 2016. The governmental experts who took part in the first UNGGE in 2004 were unable to reach a consensus and no report was adopted. The three subsequent UNGGEs were conclusive and adopted consensus reports in 2010 (UN Doc. A/65/201), 2013 (UN Doc. A/68/98), and 2015 (UN Doc. A/70/174), which have been accepted by the UNGA. The 2013 report of the third UNGGE marked a milestone because it affirmed the applicability of international law, especially the UN Charter, to cyberspace, which was subsequently reaffirmed in the 2015 report.

The participating experts in the 2016-2017 UNGGE failed to reach a consensus in June 2017, and thus they did not adopt a consensual report.[5] The negotiations failed due to paragraph 34 of

[4] Jean d'Aspremont, 'Cyber Operations and International Law: An Interventionist Legal Thought' (2016) 21 Journal of Conflict and Security Law 575.

[5] Arun M Sukumar, 'The UN GGE Failed. Is International Law in Cyberspace Doomed As Well?' (Lawfare, 4 July 2017) https://lawfareblog.com/un-gge-failed-international-law-cyberspace-doomed-well; Adam Segal, 'The Development of Cyber Norms at the United Nations Ends in Deadlock. Now What?' (Council on Foreign Relations, 29 June 2017) https://www.cfr.org/blog/development-cyber-norms-united-nations-ends-deadlock-now-what.

the draft final report, which dealt with questions related to international law, namely countermeasures, self-defense and international humanitarian law (IHL).

The 2016-2017 UNGGE was chaired by Karsten Geier, who was the Head of the International Cyber Policy Coordination Staff at the German Federal Foreign Office.[6] Despite some reported oral comments, notably during the Cyber Week Conference in Tel Aviv at the end of June 2017,[7] neither Karsten Geier nor the German government have yet published any official statement that gives their position and the reasons for the failure of the last UNGGE. Conversely, the Cuban, Russian and US ministries of foreign affairs published statements from their respective governmental experts taking part in the UNGGE and explained their positions.[8] China also reportedly rejected paragraph 34 of the draft final report, and questioned the applicability of self-defense, countermeasures and the law of armed conflicts.[9] However, China has not yet published any official statement on its position.

It must be highlighted that although the statements published by the Cuban and Russian MFAs rejected the application of self-defense, countermeasures and IHL to cyberspace, they reaffirmed their attachment to the applicability of international law to cyberspace.

---

[6] 'German Diplomat Selected to Chair UN Group of Experts on Cybersecurity' (Auswärtiges Amt (German Federal Foreign Office), 30 August 2016) https://www.auswaertiges-amt.de/en/aussenpolitik/themen/160830-vorsitz-expertengruppe-/283006.

[7] Geneva Internet Platform (GIP) and DiploFoundation, 'UN GGE: Quo Vadis?' Geneva Digital Watch newsletter (30 June 2017) https://dig.watch/DWnewsletter22.

[8] See, respectively:

- For Cuba : Cuba, '71 UNGA: Cuba at the Final Session of Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security.' (Representaciones Diplomáticas de Cuba en El Exterior, 23 June 2017) http://misiones.minrex.gob.cu/en/un/statements/71-unga-cuba-final-session-group-governmental-experts-developments-field-information.
- For the Russian Federation: Andrey Krutskikh, 'Response of the Special Representative of the President of the Russian Federation for International Cooperation on Information Security Andrey Krutskikh to TASS' Question Concerning the State of International Dialogue in This Sphere [*Ответ Спецпредставителя Президента Российской Федерации По Вопросам Международного Сотрудничества в Области Информационной Безопасности А.В.Крутских На Вопрос Информагентства ТАСС о Состоянии Международного Диалога в Этой Сфере*]' (The Ministry of Foreign Affairs of the Russian Federation, 29 June 2017) http://www.mid.ru/en/foreign_policy/news/-/asset_publisher/cKNonkJE02Bw/content/id/2804288 .
- For the United States: Michele G Markoff, 'Explanation of Position at the Conclusion of the 2016-2017 UN Group of Governmental Experts (GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security' (U.S. Department of State, 23 June 2017) http://www.state.gov/s/cyberissues/releasesandremarks/272175.htm.

[9] Elaine Korzak, 'UN GGE on Cybersecurity: The End of an Era?' (The Diplomat, 31 July 2017) <https://thediplomat.com/2017/07/un-gge-on-cybersecurity-have-china-and-russia-just-made-cyberspace-less-safe/>; Michael N Schmitt and Liis Vihul, 'International Cyber Law Politicized: The UN GGE's Failure to Advance Cyber Norms' (Just Security, 30 June 2017) https://www.justsecurity.org/42768/international-cyber-law-politicized-gges-failure-advance-cyber-norms/.

The composition and the work of the ILC offers an opportunity to continue the discussion on cyber international law, as demonstrated in this Reflection. Before turning to the advantages of referring the matter to the ILC, it is worth noting that the inability of the last UNGGE to reach a consensus should not be seen as a complete failure. On the contrary, it is a clear demonstration of the vivacity of international discussions on these questions. Following on from this, the ICJ held a similar view in the *Nicaragua* case regarding the question of the consequence of violations of norms of international law on their existence:

> If a State acts in a way *prima facie* incompatible with a recognized rule, but defends its conduct by appealing to exceptions or justifications contained within the rule itself, then whether or not the State's conduct is in fact justifiable on that basis, the significance of that attitude is to confirm rather than to weaken the rule.[10]

Temporary obstacles and failures are part of the normal negotiating process for norm-building. It also clearly shows that States recognize that international law applies to cyber activities, by framing their discussions and negotiations within this framework.

2. The Potential Role of the ILC in the Codification of the International Law Applicable to Cyber Operations

The potential work of the ILC on the international law applicable to cyber operations can be conducted under the two parallel objectives of the ILC: on the one hand, the promotion of the progressive development of international law and, on the other hand, its codification (ILC Statute, Articles 1 and 15).[11] Indeed, the first objective assigned to the ILC may be to identify existing norms of international law that are applicable and how they apply to cyber operations. This would have a twofold outcome: firstly, it would allow the codification of existing norms and the analysis of their interpretation in this specific context; secondly, it would also allow the identification of issues which may require further development of international law. I will not go into further detail here on the functioning of the ILC but I will instead focus on the potential

[10] *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v United States of America)* (Merits) [1986] ICJ Reports 14, 98, para 186.

[11] Statute of the International Law Commission, annexed to the UNGA Resolution 174(II) on the *Establishment of an International Law Commission*, UNGA Resolution 174(II) (21 November 1947). Article 1 of the ILC Statute mirrors Article 13(1)(a) of the UN Charter, according to which the General Assembly shall initiate studies and make recommendations for the purpose of encouraging the progressive development of international law and its codification.

advantages of making references to the ILC regarding the question of norms of international law applicable to cyber operations.

The following paragraphs compare the potential of referring to the ILC to the existing work of the UNGGE and the *Tallinn Manual*.

Firstly, the background legal work would be conducted by international legal experts in their personal capacity - as was the case for the *Tallinn Manual* but was not the case for the UNGGE - and would not be impaired by political considerations or the contingency of States' negotiations while not excluding States from the codification process. Indeed, States would continue to be involved in the drafting process by submitting comments on the ILC's documents. Furthermore, the adoption of the ILC's draft articles, reports and recommendations remains in the States' hands within the UN General Assembly.

Secondly, in such a scenario, the ILC would only work at codifying the *lex lata* and not at creating new norms, thereby avoiding States' fear of creating an international legal Frankenstein's monster, namely a norm-building process out of their control. Moreover, the referring UNGA Resolution would clearly define and limit the scope of the work of the ILC.

Thirdly, in analysing and codifying how existing norms of international law apply to cyberspace and cyber operations, the work of the ILC would also help identify the limits of international law and its possible loopholes. Such work may be particularly useful in identifying some specific issues relating to State's cyber activities that may need further elaboration of norms of international law. I do not take issue with adopting new norms, but such an identification would help distinguish between issues for which the existing legal framework is sufficient and those where evolution and new norms may be needed.

Fourthly, States' comments on the ILC's successive reports may be helpful in identifying States' *opinio juris* on relevant norms of international law.

Fifthly, the possible association of non-state actors. The ILC may consult UN agencies, international organizations, State organs or even non-state actors. In that sense, the ILC would be able to work at bridging the divide between States and non-state actors on these questions and it would be able to consult and take into account the views of private actors. For example, it could dialog with Microsoft on its proposals of the Digital Geneva Convention or an international mechanism for attribution[12] and determine how it may be related and relevant to its work. It may

[12] See notably: Scott Charney and others, 'From Articulation to Implementation: Enabling Progress on Cybersecurity Norms' (Microsoft 2016) 11–12 <https://www.microsoft.com/en-us/cybersecurity/content-hub/enabling-progress-on-cybersecurity-norms>; Brad Smith, 'The Need for a Digital Geneva Convention' (Microsoft, 14 February 2017) https://blogs.microsoft.com/on-the-issues/2017/02/14/need-digital-geneva-convention/. Microsoft commissioned a report from the RAND on its proposal for an international

also decide to engage with other non-state actors. On this point, the participating experts at the UNGGE in their preparatory work to the negotiation rounds may have consulted with other actors, including non-state actors, but the process remained predominantly, if not exclusively, state-controlled and state-centric.

Sixthly, the ILC may constitute one of the most representative options available. Both the *Tallinn Manual Process* and the UNGGE have been criticized for their lack of representativeness. The *Tallinn Manuel* attracted criticism due to the exclusivity in the origins of the participating experts, representing predominantly NATO Member States and following US approaches to international law. The UNGGE has been criticized for its exclusivity, namely having only experts from a very limited number of States. Indeed, the first three UNGGEs (2004, 2009 and 2012) had 15 members, the 2014 UNGGE had 20 members, and the last one had 25 members. The 25 States taking part in the 2016-2017 UNGGE were: Australia, Botswana, Brazil, Canada, China, Cuba, Egypt, Estonia, Finland, France, Germany, India, Indonesia, Japan, Kazakhstan, Kenya, Mexico, Netherlands, Russia, South Korea, Senegal, Serbia, Switzerland, United Kingdom and the United States. So far, only 38 States have participated in at least one UNGGE, which means that less than 20% of the 193 UN Members States has participated. It is worth noting that only Belarus, Germany and the five UN Security Council permanent members (China, France, Russia, United Kingdom and the United States) have participated in the five successive UNGGEs. One possible solution is to transform the UNGGE or create a new international body where all UN Member States would be able to send at least one governmental expert. The difficulty of the UNGGE process and the recent failure of only the few Member States participating to reach agreement highlight the difficulty, if not the impossibility, of having such discussions with too many participants. The UNGGE was a consensus-based process. Another possible reform measure would be to change the decision-making process from consensus-based to majority-based. However, in the light of the criticism voiced against the UNGGE, a body with a limited number of State representatives and a majority-based decision-making process may be heavily criticized for its lack of representativeness. The advantage of the ILC in terms of representativeness would be twofold: On one hand, the ILC is comprised of 34 members “who shall be persons of recognized competence in international law” (ILC Statute, Article 2) and who must all be from different States. Furthermore, the composition of the ILC should reflect the diversity of the international community (ILC Statute, Article 8). Members of the ILC are not sitting as governmental experts and do not represent any State; however, it may

---

mechanism for attribution, John S Davis and others, ‘Stateless Attribution: Toward International Accountability in Cyberspace’ (RAND 2017) https://www.rand.org/pubs/research_reports/RR2081.html.

be still criticized for its exclusivity and the fact that not all States are able to send an expert who may be familiar with their approach and practice on the subject matter. On the other hand, the association of all the UN Member States through the comment process at the UN General Assembly compensate for its limited membership and may also help the ILC's work to allow for the diversity of States' approaches and practices. I must acknowledge that the discussion on the representativeness was motivated because this issue triggered several critiques against both the *Tallinn Manual* and the UNGGE. This discussion is without prejudice as to whether or not there is a correlation between the success of such work and the representativeness of its adoption process. Increasing the representativeness of the process may lead to an increase in the number of participants in the discussion, with the risk of making it inefficient. This remark also questions what we mean by 'success', since it can mean success in reaching broad consensus or else success regarding the content of the reached result. These two understandings of success may be difficult to reconcile. Trying to reach the broader level of representativeness, and thus broader consensus, may also have the down-side effect of emptying the result of any significant content.

Seventhly, the time dimension of the ILC process and its potential to be pursue a work-in-progress approach. This would be a clear advantage, especially when compared to the *Tallinn Manual Process* and the UNGGE. In the case of the *Tallinn Manual Process*, some States were invited to comment on the draft of the second edition, notably through the *Hague Process*. Two points must be made here: firstly, since the *Tallinn Manual Process* is an experts' exercise, the State may not have contributed as extensively as if it was a codification process; secondly, and more importantly, this was a one-time consultation and thus it did not create the conditions for a developed dialog between the consulted States and the participating experts. In the case of the UNGGE, the process had to be restarted following the establishment of each new UNGGE. Thus, unlike the *Tallinn Manual Process*, it could have led to the establishment of a long-term discussion between the UNGGE and the UN General Assembly, but it appeared to be limited by and captive of international politics. In the case of the ILC, as mentioned above, the ILC would produce draft articles on which States can comment, and then it will rework them until both the ILC and States reach agreement. One of the down-sides of such a process is that it would take several years or possibly even decades. At the same time, however, it may create the conditions for dialog between the ILC and States, between States themselves and specific questions on the matter. Moreover, even before the adoption of a final version by the ILC and the UN General Assembly, the successive drafts and reports may already be useful for the interpretation of the international law applicable to cyber operations. On this point, the ILC's

Articles on Responsibility of States for Internationally Wrongful Acts offer an apt illustration. The ILC worked for more than three decades on the topic but the successive reports were already valued, referred to and commented on before the adoption of the final version in 2001,[13] contributing to the process of interpretation and codification on the customary international law on the matter. Finally, on the time-dimension of the process, it is worth highlighting that cyber operations are a recent phenomenon, and recourse to international law by States to analyse and respond to cyber threats is really only just beginning. After some embryonic references, the international legal framework has actually been used for the first time regarding the 2015 Sony Picture hack and the attribution of this incident to North Korea by the United States, which then undertook self-help measures. This practice developed in recent years, most notably in the cases of the cyber incidents during the 2016 US and 2017 French elections and WannaCry. Thus, the length of the ILC process may also be beneficial for it gives States the time to develop their approach and practice, as well as for the ILC or any other body to assess State practice and interpretation of international law on these questions.

Concluding Remarks

This Reflection has invited the reader to consider a new possible forum to continue the international discussions and negotiations on cyber international law, namely referring the question of the interpretation of the international law applicable to cyber operations to the ILC. It has highlighted that the ILC would offer an appropriate platform to involve both States and non-state actors, and to take into account the diversity of approaches to the issue. That being said, we should not be naïve: the ILC does not constitute a panacea to the increasing threats to the international peace and stability of cyberspace. Indeed, norms of international law, and consequently the work of the ILC, are not able to solve all the issues related to state-sponsored cyber operations. Moreover, despite offering some interesting features, especially if compared to other existing solutions, referring the matter to the ILC is not exempt from downsides and is open to the general criticisms of the ILC.[14] In this sense and when compared to the UNGGE or the *Tallinn Manual Process*, the ILC may constitute a solution although an imperfect one.

[13] Articles on Responsibility of States for Internationally Wrongful Acts (adopted by the International Law Commission at its fifty-third session in 2001, annexed to General Assembly resolution 56/83 of 12 December 2001, and corrected by document A/56/49(Vol I)/Corr4).

[14] See generally: Georg Nolte (ed), *Peace through International Law: The Role of the International Law Commission. A Colloquium at the Occasion of Its Sixtieth Anniversary* (Springer 2009); Pemmaraju Sreenivasa Rao, 'International Law Commission', *MPEPIL* (2017).

Cite as: François Delerue, ‘The Codification of the International Law Applicable to Cyber Operations: A Matter for the ILC?’, ESIL Reflections 7:4 (2018).