INTERNATIONAL LAW IN CYBERSPACE: ARE WE ASKING THE RIGHT QUESTIONS?

Statement delivered by Dr Francois Delerue - Research Fellow in cyber defense and International Law at the IRSEM (Institut de Recherche stratégique de l'École militaire)

Intersessional multi-stakeholder meeting of the Open-ended Working Group

CHECK AGAINST DELIVERY

Mr Chairman,
International law, and in particular the Charter of the United Nations, are the backbone of international relations and are crucial for maintaining international peace and security. From this perspective, it is important to note that the applicability of international law to cyberspace and cyber operations has been a matter of controversy. The contentious question was whether cyberspace constitutes a new 'Wild West' where existing norms of international law, if not international law itself, would not be applicable and thus would not regulate the activities taking place in this 'space'. This question has been settled in both the academic literature as well as in State practice: international law applies to cyberspace and cyber operations. Yet, international law remains one of the focuses of the international discussions and works on international peace and security in cyberspace. One may wonder why. The reason is because having agreed on the applicability of international was only the first step. The second step is determining how international law applies. Consequently, the question then became determining the specific interpretation and application of the norms of international law to cyberspace and cyber operations. The application of specific norms and principles of international law remain matter of disagreement and contestation between states.

The articulation between these two questions is perfectly illustrated by the evolution of the work of the United Nations Groups of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (UNGGE). It is worth noting that it had been recognized in the consensual reports of the two previous UNGGE in 2013 (UN Doc. A/68/98) and 2015 (UN Doc. A/70/174), and that several States confirmed this position in their comments on these reports and in their national cyberdefense and cybersecurity strategies. The fifth UNGGE, however, failed on the very question of the application of specific norms of international law, namely self-defense, countermeasures and the law of armed conflicts. In 2018, the General Assembly of the United Nations requested the establishment of two new processes that are currently ongoing, a new UNGGE

(Resolution A/RES/73/266) and an Open-Ended Working Group (OEWG – Resolution A/RES/73/27). International law is part of the mandate of both processes.

This situation leads us to introduce a third question. The questions on the applicability of international law and on the norms of international law apply may be seen at the two faces of the same coin. Yet, reflecting on these questions lead to wonder on the delineation of the concerned norms of international law. In other words, this third question focuses on the determination of which norms of international law should be applied and what is their content and limits. Conversely to domestic law, the vast majority of the norms of international law is vague, offering to the subjects of international law a high level of flexibility and adaptability in the interpretation and application of these norms. Building on these observations, the central question on the delineation of the norms of international law applicable to cyber operations is the determination of where should be placed the cursor between what need to be agreed between States and what should be left for the unilateral interpretation of each State. I believe that this third question is too often left aside in the international discussions the international law applicable to cyber operations while it is of equal importance in comparison to the discussion on the content and interpretation of norms of international law.

To illustrate this third question, we may draw a parallel with a manual on norms of international law, such as the Tallinn Manual on the International Law Applicable to Cyber Operations (Cambridge University Press 2017), a similar question is to be asked: the distinction between what should be settled and enshrined within the rules and what should be left for interpretation and thus only developed in the commentary under the rules. In this illustration, the 'rules' being what should be agreed by the international community while the 'commentaries' would be what could be left to the unilateral interpretation of each States. Two further aspects must be highlighted on what should be agreed collectively by the States. Firstly, the quest of a consensus on the interpretation of specific norms of international law may also be achieved through non-binding norms. Secondly, when assessing what should be agreed and thus further develop in international law, it is necessary to determine whether this should be done at the universal, multilateral, regional or bilateral level.

This third question resonates with the two main challenges regarding the application of international law to cyberspace: firstly, given the unique characteristics of cyberspace, interpreting the application of the norms of international law to cyber operations may require a certain level of adaptation, not transformation. Secondly, the subjects of international law, and particularly States, may have different if not divergent interpretations of certain specific norms of international law. In that perspective, more and more States are expressing publicly their approach to international law.
The Resolution establishing the sixth UNGGE (Resolution A/RES/73/266) requests the participating States to submit national contributions on their views on how international law apply to cyberspace. It is necessary, however, that more States, notably those which are not taking part in the UNGGE, expose their views publicly on how international law apply to cyberspace and cyber operations. In that perspective, the OEWG may serve as an important platform for States to present and discuss their approaches. Moreover, the development of such practice is also important for capacity building, in allowing the identification of the specific needs in terms of legal and strategic cooperation.

The principle or rule of State sovereignty offers a perfect case study for this third question. Indeed, this principle or rule as multiple dimensions on which it is necessary to determine if whether a consensus is needed and if such a consensus exists, or whether these dimensions can be left unsettled and defined unilaterally by each State.

Firstly, the nature of 'sovereignty' is not settled, some States and scholars consider it is a principle while other it is a rule of international law. For instance, France recently defined it as a rule of international law while the United Kingdom consider it only as a principle.

Secondly, there is no consensus on its extent, that is to say on what constitutes State sovereignty over cyberspace.

Thirdly, a diversity of approaches exists when it comes to characterizing a violation of territorial sovereignty through cyber operations. There are three main views on this question according to which:

1. Any cyber operations penetrating a foreign system constitutes a violation of sovereignty. This is for instance the French approach;
2. A cyber operation penetrating a foreign system constitutes a violation of sovereignty only if it meets a threshold of harm. This is for instance the approach adopted in the Tallinn Manual 2.0 and by the United States;
3. Territorial sovereignty cannot be breached by a cyber operation unless it constitutes a violation of the principle of non-intervention. This is for instance the British approach.

The example of sovereignty demonstrates the diversity of acceptation of States and scholars on a specific norm of international law. Following on the previous observations, the question is then to determine what dimensions of sovereignty should be agreed collectively by the States and what dimensions should be left to the interpretation of each State.

To conclude, it should be highlighted that the observations made in this contribution have a particular resonance regarding the current debate on the need for a treaty on the international law applicable to cyber operations. The challenges arising from both the unique characteristics of cyberspace and the different if not divergent interpretations of certain specific provisions of international law have led some States and commentators to suggest that the international community should move to adopt an international treaty. The adoption of a new legally binding instrument may be justified, in the future, by the identification of specific problems that cannot be solved by the lex lata. However, in addition to the identification of the gaps in international law, it will be necessary to determine whether they should be filled by the adoption of new consensual norms of international law, through non-binding agreements, or left to the unilateral interpretation of each State.

IRSEM
INSTITUT DE RECHERCHE STRATÉGIQUE DE L'ÉCOLE MILITAIRE

Dr François Delerue is a research fellow in cyberdefense and international law at the IRSEM (Institut de Recherche stratégique de l'École militaire), an adjunct lecturer at Sciences Po Paris and a rapporteur on international law to the Academic Advisory Board of the EU Cyber Direct Project. His book titled Cyber Operations and International Law is forthcoming with Cambridge University Press. He also designed a flowchart on how to apply the norms of international law to cyber operations.