POLICY IN FOCUS

THE APPLICATION OF INTERNATIONAL LAW IN CYBERSPACE: IS THERE A EUROPEAN WAY?

François Delerue, Joanna Kulesza and Patryk Pawlak*
April 2019

International law, and in particular the Charter of the United Nations, is the backbone of international relations and is crucial for maintaining international peace and security. Despite this, the application of international law to cyberspace and cyber operations has been a matter of controversy. The contentious question has been whether cyberspace constitutes a new "Wild Wild West" or whether existing international legal provisions provide sufficient guidance and guarantees for states' relations in cyberspace. This question has been settled both theoretically in academic literature as well as by state practice: International law applies to cyberspace and cyber operations. This conclusion has also been reiterated in the 2013 and 2015 consensual reports of the previous United Nations Groups of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (UNGGE). Several states have also confirmed this position in their comments on these reports and in their national cyberdefence and cybersecurity strategies.

The affirmation that international law applies to cyberspace and cyber operations within the UN-led process has laid the foundation for other regional processes. Consequently, the question has evolved from "whether" to "how" international law applies in cyberspace – with a growing focus on determining the specific interpretation and application of the norms of international law to cyberspace and cyber operations. In fall 2018, the UN General Assembly (UNGA) adopted two resolutions setting in place new platforms where questions of international law would be debated. The first was a new UNGGE and the second an Open-Ended Working Group (OEWG).[1] Both resolutions recognise that international law, and in particular the Charter of the United Nations, applies to cyberspace, based on the 2013 and 2015 UNGGE reports.

International law in cyberspace: state of play

The interpretation of international law regarding its application to cyberspace is an important aspect of cyber diplomacy. Disagreements over legal issues were the key element that contributed to the failure of the 2016/2017 UNGGE. The biggest source of contention was paragraph 34 of the draft final report, which dealt with questions related to international law, specifically countermeasures, self-defence and international humanitarian law (IHL).

Despite the lack of consensus over the text, the UNGGE has provided a much-needed platform for debates over questions linked to the application of international law in cyberspace. Two issues in particular continue to pose a challenge:

* The content of this publication does not reflect the official opinion of the European Union. Responsibility for the information and views expressed therein lies entirely with the author(s).

[1] The Russia-sponsored resolution titled Developments in the field of information and telecommunications in the context of international security (A/RES/73/27) and the US-sponsored resolution titled Advancing Responsible State Behaviour in Cyberspace in the Context of International Security (A/RES/73/266).

1. Different approaches exist, in both academic literature and states' approaches, for whether a cyber operation may constitute a breach of territorial **sovereignty.** There are three main viewpoints, according to which, a) any cyber operation penetrating a foreign system constitutes a violation of sovereignty; or b) a cyber operation penetrating a foreign system constitutes a violation of sovereignty only if it meets a threshold of harm. This is the approach adopted in the Tallinn Manual 2.0, for instance, and by the United States[2]. The third viewpoint holds that c) territorial sovereignty cannot be breached by a cyber operation unless it constitutes a violation of the principle of non-intervention. This is the British approach[3]. Consequently, it appears states will have to continue their reflection upon the extent of territorial sovereignty in cyberspace.

2. The failure of the 2016-2017 UNGGE highlighted the diversity of opinions among states regarding which **unilateral measures** may be adopted by a state in response to cyber operations in accordance with international law. This is because some countries oppose the application of norms of **self-defence and countermeasures**. Self-defence may be applicable only in a very limited number of cases. There is broad consensus that no cyber incident to date has justified self-defence in terms of international law. Conversely, many more cases of cyber operations could be considered "internationally wrongful acts" (e.g. a violation of territorial sovereignty, a breach of the principle of non-intervention, significant transboundary harm, etc.) to which a response could be the adoption of countermeasures (e.g. counter-cyber operations). It is thus necessary to continue the discussion with the aim of determining how states approach the available responses to unlawful cyber operations.

Furthermore, there are two broader challenges when it comes to applying the principles and provisions of international law to cyberspace. First, given cyberspace's unique characteristics, interpreting international law that is applicable to cyber operations may require a certain level of adaptation, not transformation. Second, the subjects of international law, particularly states, may have different – if not divergent – interpretations of certain specific provisions of international law. Such challenges have led some states and commentators to suggest that the international community should move to adopt an international treaty. However, as past experiences suggest, such an approach is not a viable solution in cyberspace, at least for the time being. The United Nations Convention on the Law of the Sea (UNCLOS) – often cited by the treaty's supporters as a model – is not a viable example and cannot be transposed to cyberspace. As a matter of fact, UNCLOS was made possible by decades of practice and discussions between states, allowing these elements to be used as a basis for the preparation and negotiation of the treaty. That time and dialogue is clearly missing in the cyber context; therefore, initiating the negotiation of a treaty would be premature. Only with continued first-hand experience by states and discussions on how international law applies to cyberspace will it be possible to identify eventual gaps in existing international law, which may require adjusting international law and norms in the future.

Transboundary harm and cybersecurity due diligence

While international law is binding to states, it cannot be enforced directly upon non-state actors, who can be either victims or perpetrators of an attack. With that in mind, the question of how the international community as a whole can effectively ensure compliance with international law by non-state actors – who operate within the jurisdiction of states that are either reluctant to introduce or enforce appropriate national laws or that lack the capacity to do so – remains open.

Attacks against critical infrastructure, especially by way of cybercrime, is but one of the new additions to the universal catalogue of known threats to international peace and security that has developed over centuries. Before cybersecurity became the primary focus, similar debates took place in the areas of nuclear power, oil production and transportation and outer space exploration. This triggered a shift in the way the global community looked at international liability and state responsibility. The challenges those areas of activity brought about resulted in a state duty to protect others from transboundary harm, i.e. detrimental activity that originates within one state's territory or jurisdiction yet affects another's territory or subjects. It was exactly this challenge that kept the UN International Law Commission (ILC) occupied for over 60 years as it tried to answer the questions of state responsibility and

[2] Brian J Egan, 'Remarks on International Law and Stability in Cyberspace' (US Department of State 2016). Available at: https://2009-2017.state.gov/s/l/releases/remarks/264303.htm

[3] Jeremy Wright, 'Cyber and International Law in the 21st Century' (UK Attorney General's Office 2018). Available at: https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century.

international liability for transboundary harm. This was done primarily by detailing the duties states have to implement standards for private bodies in order to prevent significant harm to "neighbouring" countries.[4] A crucial element of this puzzle has been the issue of due diligence – a flexible international standard, indicating what actions states need to perform to ensure private sector compliance and prevent significant transboundary harm. The ILC's work indicates that when performing any obligation of conduct – one that requires them to perform in a certain way as opposed to achieving a particular result – states need to act with due diligence.

This flexible standard covers nine elements[5]:

- Good faith on behalf of the state in meeting its international obligations, the duty to prevent significant transboundary harm;
- Due diligence is the result of the well-recognised **principle of good neighbourliness**, which requires states to refrain from causing harm or damage within the territory or to the legally protected interests of others or in common territories;
- Performance of any due diligence obligation is **assessed territorially**, i.e. with regard to a given territory and any potentially harmful actions initiated or conducted therein;
- The duty to perform with due diligence is a **derivative of the principle of sustainable development**. As such, it requires a risk assessment for any new procedure or legislation that may bring with it a risk of significant transboundary harm;
- As confirmed in numerous international legal treaties, the due diligence principle is a **state obligation to undertake "all necessary measures" expected of a "good government" in a given situation**. A state is to perform according to this standard when meeting its international obligations, but the individual measures – and the tools for assessing them – are always case-specific. Due diligence, however, always implies a need for administrative or other formal procedures to authorise risk-generating activities undertaken within a state's territory, jurisdiction or control. These procedures need to be enforced in the same way that a "good government" would enforce them. When trying to identify how a "good government" would have acted, the court is to consider, among other case-specific factors, the performance of state bodies in the state's own affairs, the state's economic condition and the performance of countries in the region or in a particular economic sector. Courts often rely on the assessment of experts in a given field when attempting to identify what actions should have been taken by a government to prevent harm, as discussed below;
- **Assessing the due diligence standard relies on technical expertise and reference to the state of the art in a given area of practice.** With that in mind, individual efforts are usually set against the financial and technological capabilities of the acting state. Precautions that are taken must reflect the current state of technical knowledge in a given area; nothing that is clearly outside the financial or organisational capability of the state (or states in its region) can be required. The efforts taken by the acting state are set against similar measures taken by other states in the region in given circumstances. Also, the size of potential damage is to be considered: The more severe the pending harm, the more intensive state efforts are expected to be;
- **Due diligence also encompasses the duty to exchange information with others**, including states, private parties and international organizations. Information on potential risks and measures taken to mitigate them is to be shared, with the exception of information considered crucial to state security or a country's economic interests. This thin line between information that is necessary for others to effectively protect themselves from pending grave damage and information that is considered crucial to a state's economy is always drawn by the risk-generating state; it is among the most disputed issues in today's globalised economy. There are no universal standards for drawing this line between what needs to be shared for the purposes of global security and what is allowed to be kept secret even when global security is at stake;

[4] In this case, "neighbouring" was defined as any country potentially affected by risk-generating activities performed within state territory or under state jurisdiction or control.

[5] ILC Report, 2001, U.N. Doc. A/56/10, att. 10, 38–39; ILC, Second report by F.V. Garcia Amador, Special Rapporteur; International responsibility, 1957, U.N. Doc. A/CN.4/106; ILC Report, 2001, U.N. Doc. A/56/10, att. 10, which includes the 2001 ILC Draft Articles on State Responsibility, 59–365 as well as the 2001 ILC Draft articles on prevention, 366–435. For a detailed discussion see also: Barboza's 12th report, 1996, U.N. Doc. A/51/10; ILC Report, 1994, U.N. Doc. A/49/10. See also: Robert P. Barnidge Jr., 'The Due Diligence Principle Under International Law' (2006) 8 ICLR 81 ff.; Riccardo Pisillo Mazzeschi, "The 'Due Diligence' Rule and the Nature of the International Responsibility of States" (1992) 35 GYIL 9–49.

- **States are required to refrain from discrimination** when it comes to the treatment of both victims and operators. States shall disregard their country of origin, the role they played in the potentially harmful activity and their economic status. A bias toward certain national operators, for instance, and holding them to a different standard than foreign ones, would be considered a violation of the due diligence standard;

- **States' obligation to due diligence is continuous, requiring them to maintain their efforts in assessing and preventing international law violations that could result in potential harm to others**. A single risk assessment performed before or at the start of a risky activity would not be considered diligent, nor would a single authorization procedure or one done occasionally. Potentially harmful activities need to be continuously monitored and operators' procedures must be updated according to the latest technological expertise and information received from other parties.

International legal scholarship and practice indicate that due diligence is not to be considered with regard to so-called ex post facto prevention, i.e. measures taken after actual damage arises. Moreover, there is no consensus on the vicarious responsibility of states or their risk liability for the actions of individuals, unless necessary stipulations are put into an international treaty that is binding for the acting state. With that in mind, the international law principles of due diligence remain a practical and flexible tool for assessing the efforts that states take to prevent harmful actions in cyberspace.

Recent developments in the European Union

The EU has stressed on multiple occasions the importance of a "global, open, free, stable and secure cyberspace where human rights and fundamental freedoms and the rule of law fully apply for social well-being, economic growth, prosperity, and integrity of our free and democratic societies".[6] In this context, it firmly condemns the malicious use of Information and Communications Technologies (ICTs) to cause economic loss, undermine citizens' trust in the internet and foment instability in state-to-state relations. While it is ultimately the prerogative of individual EU member states to decide how they want to respond to specific incidents, and even though such responses may have to be far-reaching out of self-defence, no actor can address the vulnerabilities in cyberspace on its own. This is why EU institutions and member states have acknowledged the value of acting collectively. Consequently, the EU has pursued a two-legged approach focused on strengthening accountability and resilience in cyberspace.

Strengthening accountability

In order to strengthen adherence to norms for responsible behaviour in cyberspace as they are enshrined in the 2013 and 2015 UNGGE reports, and to reduce impunity resulting from the violation of international law or domestic criminal laws, the EU adopted in 2015 a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities – commonly known as a "Cyber Diplomacy Toolbox".[7]

The EU strongly upholds that the "existing international law is applicable to cyberspace" and emphasises that "respect for international law, in particular the UN Charter, is essential to maintaining peace and stability"[8] and that "malicious cyber activities might constitute wrongful acts under international law".[9] In that respect, following the NotPetya and WannaCry attacks, the EU has stressed that "States must not use proxies to commit internationally wrongful acts using ICTs, and should seek to ensure that their territory is not used by non-state actors to commit such acts".[10] In addition, the EU frequently emphasises that states "should not conduct or knowingly support ICT activities contrary to their obligations under international law, and should not knowingly allow their territory to be used for malicious activities using ICTs".[11] Both these elements are clearly based on the consensus enshrined in the 2015 UNGGE report, which as such should constitute the basis for further discussions.

The EU also acknowledges that a state-victim of an act that constitutes an internationally wrongful act may, under certain conditions, resort to proportionate countermeasures as stipulated in international law. In cases of activities that amount to a use of force or an armed attack within the meaning of the UN Charter, states may choose to exercise their inherent right of individual or collective self-defence as recognised in Article 51 of the UN Charter. In such cases, member states may also choose to invoke articles 42(7) of the

[6] Council of the European Union (2018) *Council conclusions on malicious cyber activities*, 16 April 2018.
[7] Council of the European Union (2017) Council conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities, 19 June 2017.
[8] Council of the European Union (2018).
[9] Council of the European Union (2017).
[10] Council of the European Union (2018).
[11] Ibid.

Treaty on the European Union (the so-called "Mutual Defence Clause").

Strengthening cyber resilience

In light of the limitations resulting from the lack of international consensus on the application of existing international law in cyberspace, the EU has also taken steps aimed at strengthening state and societal resilience in Europe and beyond its borders. This is partly linked to the fact that – in addition to contributing to economic growth and human development in general – high levels of cyber resilience ultimately contribute to increasing the threshold for what might constitute an armed attack in cyberspace. They also generate a higher standard for what would be considered a proportionate response. To that end, due diligence has become a substantial element of recent EU lawmaking, in particular through the Network and Information Security (NIS) Directive and General Data Protection Regulation (GDPR). Both documents introduce the flexible blueprint of good community practice as the standard for securing crucial data and infrastructures.

- As per the NIS Directive Article 14, member states are to "ensure that operators of essential services take **appropriate and proportionate technical and organisational measures** to manage the risks posed to the security of network and information systems which they use in their operations. Having regard to the state of the art, those measures shall ensure a level of security of network and information systems appropriate to the risk posed" [emphasis added]. The reference to "appropriate measures" is a direct allusion to the due diligence principle in international law. This benchmarking of good practices is well present in other cooperation mechanisms introduced by the NIS Directive.[12]
- Similarly, the GDPR introduces, for example, a "data protection impact assessment," which obliges the controller to take "**reasonable means in terms of available technologies and costs of implementation**" to mitigate all risk to personal data in the disposal thereof [emphasis added]. It also emphasises the role of extra-legal standard setting encouraging "associations or other bodies (...) to draw up codes of conduct (...) to facilitate the effective application" of the Regulation. Such codes of conduct are to "calibrate the obligations of controllers and processors, taking into account the risk likely to result from the processing for the rights and freedoms of natural persons", later serving as points of reference for expected standards of professional behaviour.[13]

In addition, the EU has been supporting efforts at strengthening the cyber resilience of other countries, both through bilateral cyber capacity-building programmes and the support provided to projects implemented by other organisations, such as the Council of Europe. The particular focus of these projects is on strengthening countries' mechanisms for fighting cybercrime, in particular through ratification of or approximation of their legislation to the Budapest Convention on Cybercrime. The EU is also an active member of the Global Forum on Cyber Expertise – a multi-stakeholder platform with the aim of improving international cooperation on cyber capacity building, consequently strengthening global resilience.

The way forward

In light of the above considerations, there are three possible avenues through which the EU and its member states can contribute to advancing the discussion about the application of international law to cyberspace.

1. **Transparency framework**: While concrete decisions remain the competence of each member state, the EU should encourage its members to develop and publicly disclose their approach regarding the application of international law to cyberspace. The public disclosure of these elements would be relevant for the international discussions and cooperation on these matters at the universal, regional and bilateral level. The adoption of norms of behaviour, non-legally binding by nature, is also particularly relevant since some of them are interpreting existing norms of international law. These elements, the publicly released approaches and norms of behaviour, would be particularly useful in identifying the opinio juris of states. Defining the elements of a joint transparency framework regarding the application of

[12] Council of the European Union (2016) Directive (EU) of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union. See specifically Chapter IV.

[13] Council of the European Union (2016) Regulation (EU) 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). See preamble, para. 94, 98 and 99.

international law in cyberspace – including further discussion about the principle of due diligence, sovereignty or countermeasures – could be particularly useful in light of the UNGGE and OEWG that will be launched.

2. **Legal capacity building:** Past experiences demonstrate that the knowledge of international law and its relevance for cyberspace remains very limited. This poses a risk to stability in cyberspace as it increases the risks of overreaction, limits states' understanding of their existing obligations and commitments and limits states' capacity for a more effective response. Consequently, there is a clear need for exploring different avenues for improving the understanding of these issues among governments. This includes a better understanding of the role that civil society organisations and research institutes play in the process, in particular through legal training. Here again, the EU and its member states can play a very important role, either by focusing explicitly on legal capacity building or by incorporating relevant aspects of existing international law into ongoing and planned cyber capacity-building projects, such as in the domain of cybercrime or resilience. Such approaches would help ensure that a respect for international law and norms in cyberspace is ensured through domestic laws and regulations from very early on.

3. **Best practices and lessons learned:** Building resilient societies remains the most effective way of decreasing the risk of conflict. Given that different states have adopted different approaches to increasing their own resilience, it is desirable to map those policies and practices that have a direct link to the discussion of the application of international law. As mentioned above, several pieces of legislation passed by the EU offer a good example of how certain provisions of domestic law are directly linked to international law. In that sense, the creation of a CERT or adoption of a cybersecurity strategy can be viewed as examples of state's due diligence. Including such requirements in the domestic legal order ultimately contributes to increasing their enforcement. Mapping similar practices in other countries could provide more clarity and further enhance transparency in cyberspace.

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

Dr Joanna Kulesza is an Assistant Professor in International Law at the Faculty of Law and Administration, University of Lodz.

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

This project is funded by the European Union.