A Wild Wild Web? Law, norms, crime and politics in cyberspace

by Patryk Pawlak

Following the Council Conclusions on Cyber Diplomacy adopted in February 2015, the decision by the EU Ministers of Foreign Affairs to endorse the development of a framework for a joint EU diplomatic response to malicious cyber activities – the so-called Cyber Diplomacy Toolbox (CDT) – represents another step in strengthening the EU's position as a 'forward-looking cyber player'. The EU's leadership in promoting 'an open, free, stable and secure cyberspace' is now more critical than ever before.

The discussion about states' sovereignty in cyberspace is intensifying while progress towards a stability regime for the digital domain – based on norms, international law, and confidence building measures – remains slow. This is hardly surprising given that many states increasingly see cyberspace as an environment in which they can pursue their strategic objectives free of the constraints posed by physical borders. The EU's recognition of the need for a common and comprehensive response signals that the Union intends to make a better use of existing diplomatic tools in defence of its interests and values.

International law and cyber stability

Does current international law apply to cyberspace, or is a new cyber convention needed? This question has been debated by lawyers and policymakers since 1998, when the UN adopted the first (Russia-sponsored) resolution on 'developments in the field of information and telecommunications in the context of international security'. Different actors have given different answers to this question, and it still remains one of the key sticking points in the emerging global cyber stability regime.

The 2013 United Nations Group of Governmental Experts (UN GGE) report clearly stated – for the first time – that 'international law, and in particular the Charter of the United Nations, is applicable and is essential to maintaining peace and stability and promoting an open, secure, stable, accessible and peaceful ICT environment'. Since then, most efforts have focused on trying to understand how the existing body of law can be interpreted in a cyber-specific context. A non-exhaustive list was incorporated in the 2015 UN GGE report and included a state's obligation to observe principles such as sovereignty, sovereign equality, the peaceful settlement of disputes, and non-interference in the internal affairs of other states.

The experts also concluded that states must not use proxies to commit intentionally wrongful acts using ICTs, and should seek to ensure that their territory is not used by non-state actors to do the same. The work of the UN GGE was later reflected on

in other international groupings: the G7 Ministers of Foreign Affairs who called on states to publicly explain their views on how existing international law applies to state activities in cyberspace, for example.

The Tallinn Manual 2.0 – a comprehensive analysis of the international law applicable to cyberspace both in peacetime and during a conflict drafted by the International Group of Experts at the NATO Cooperative Cyber Defence Centre of Excellence – took the debate a step further. The Manual identifies 154 'black letter laws' governing relations between states in the digital domain. The main conclusion reached by the authors is that cyber events 'do not occur in a legal vacuum and thus states have both rights and bear obligations under international law'. Even though the group was gradually expanded to ensure the variety of views and the transparency of its proceedings through the so-called Hague Process, the Manual is viewed as a primarily academic product without any binding implications for governments.

The EU position expressed in the European Cybersecurity Strategy and numerous Council Conclusions is clear: existing international law applies in cyberspace. This implies that under the general principles of international law states have an obligation to ensure that their territory is not used for intentionally wrongful acts using ICTs (due diligence principle). The EU's efforts so far have focused on building an international consensus on the application of existing international law to cyberspace (through the Tallinn Manual process, among other initiatives), developing voluntary non-binding norms of responsible state behaviour based on the work of the UN GGE, and supporting regional initiatives by the Organisation for Security and Co-operation in Europe (OSCE), ASEAN Regional Forum (ARF) and Organisation of American States (OAS) on confidence building measures. However, the decision to develop a Cyber Diplomacy Toolbox is an important step in the EU's evolving cyber posture.

'The EU position expressed in the European Cybersecurity Strategy and numerous Council Conclusions is clear: existing international law applies in cyberspace.'

But not everyone shares this interpretation. Russia's Information Security Doctrine, adopted in December 2016, acknowledges that universally recognised principles and norms of international law form the legal framework of the doctrine but does not include any specific reference to whether or not existing laws apply to cyberspace. Similarly, China's International Strategy of Cooperation on Cyberspace (released last February) merely contains a commitment to 'study the application of international law in cyberspace from the perspective of maintaining international security, strategic mutual trust and preventing cyber conflicts'. This is not surprising given that since 2011, under Sino-Russian leadership, members of the Shanghai Cooperation Organisation (SCO) have been working on a draft International Code of Conduct for Information Security that is broadly seen as a direct challenge to the vision promoted by the EU, US and other like-minded countries. The SCO's draft Code of Conduct received a cold reception not only because of its content (concerning the right to privacy and other fundamental freedoms, for example) but also due to the risk of it becoming a launching pad for a new UN-negotiated convention.

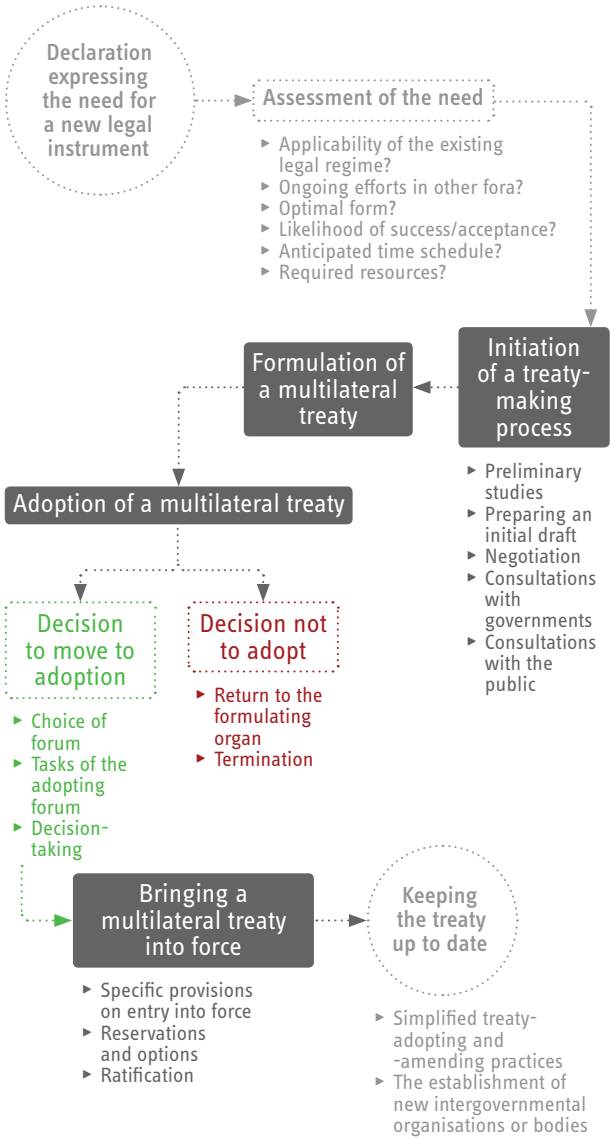
In that context, and in light of the associated political risks, it is problematic that the calls for a new international legal instrument that 'would protect citizens and businesses from malicious state-run cyber operations' are now also coming from the private sector. For instance, Microsoft's proposal for a 'Digital Geneva Convention' that commits governments to protecting civilians from state attacks is an idea that gained some traction in the media and the research community despite being in clear contradiction with a broadly accepted view that the existing international law applies to the cyber realm. Any deviation from this approach, at the current stage, could pose a serious challenge to stability in cyberspace.

International law and cybercrime

The narrative about a new legal instrument has been spreading also with regard to the fight against cybercrime.

Currently, the Council of Europe Convention on Cybercrime adopted in 2001, known as the Budapest Convention, is the only legally binding instrument providing a framework for international cooperation in the fight against cybercrime. Promoted by the EU and a group of like-minded states and organisations, the Budapest Convention has served as a benchmark for setting global standards in the fight against cybercrime and access to electronic evidence. It has also become a reference

The international treaty-making process



Data: United Nations University

point for other regional initiatives such as the 2014 African Union Convention on Cyber Security and Personal Data Protection (the Malabo Convention), and a source of inspiration for many countries developing their own national cybercrime legislation – albeit with a varied degree of compatibility.

At the same time, certain countries either reject the conventions (Russia) or challenge its global aspirations based on a non-inclusive process through which it was negotiated (India, Brazil). The calls for a new international cybercrime instrument are a direct consequence. The Open-ended Intergovernmental Expert Group on Cybercrime (IEG), established in 2010 by the UN Congress on Crime Prevention and Criminal Justice (CCPCJ), was tasked with preparing a 'comprehensive study' examining different options for strengthening international efforts in the fight against cybercrime.

A draft study presented by the United Nations Office on Drugs and Crime (UNODC) in 2013 has put forward seven options, including the development of multilateral tools for international cooperation regarding electronic evidence in criminal matters and a comprehensive instrument on cybercrime. The findings were a boon for China, Russia, Brazil and South Africa – but also for countries like Iran, Sudan, Cuba, Algeria or Guatemala – who used the recent meetings of the IEG to promote the idea of a new convention on cybercrime.

The final outcome has resulted in a carefully crafted balance on the language concerning the status of the study and the future work of the expert group instead of focusing on a new instrument – partly due to the increased number of countries advocating in favour of the Budapest Convention and the lack of consensus among the G77. However, the Russian-led calls for a UN General Assembly vote on a new treaty continued at the CCPCJ meeting in May, and are very likely to grow louder next year when the attention will be on cybercrime specifically.

Multilateralism and the politicisation of law

Over the years, the discussion about new legal instruments for cyberspace has become increasingly politicised. The main dividing line lies between the countries which insist on state sovereignty in cyberspace and those which interpret such calls as way to ensure state control over the internet. Paradoxically, the United Nations system – established as the backbone of multilateralism – is increasingly being used by certain states as a vehicle for furthering their national interests in cyberspace. This, in turn, undermines the UN's credibility as a venue for cyber-related debates. For this reason, and in light of the complexity of the UN treaty-making process, starting a debate about new legal instruments regulating cyberspace seems to be premature: merely defining the scope of a new legal instrument would be a complicated task. At the same time, the international legal landscape is already awash with treaties not yet in force or abandoned due to their limited ratification.

Given the pace of technological progress and the time it would take to negotiate any new international instrument, it is fair to assume that the inevitable gap between the initial expectations and the final outcome would be huge – and a source of disappointment. Historically, conventions regulating other domains such as space, air and sea have undergone long negotiations before their signing and entry into force. For instance, the United Nations Convention on the Law of the Sea (UNCLOS), a regime detailing rules governing all uses of the oceans

and their resources, was opened for signature in December 1982, after 14 years of negotiations, and came into force only in 1994. Altogether, it took 26 years before the Convention started to regulate international sea behaviour – and the text is still subject to amendments.

The Budapest Convention, on the other hand, was opened for signature in 2001 – four years after the negotiations were launched – and came into force in 2004. As of June 2017, 55 countries worldwide have signed and ratified the Convention – but the average time between signature and entry into force is still almost six years.

Negotiations on a new convention would certainly benefit some state actors, but not necessarily the broader cyber community. Because international treaties are negotiated between states, non-state actors – including civil society organisations and the private sector – would have very limited scope to influence the process. This would thus entail the dangerous risk of shifting the multi-stakeholder nature of internet governance towards a primarily state-centric model and would further endanger the open and free nature of the internet. Although non-state actors have often been important players in raising awareness about international security issues (a role explicitly recognised in Article 71 of the UN Charter), their role in treaty negotiations is usually limited to a consultative one at best.

Alternative futures

A fading consensus on the application of existing international law to cyberspace sends a clear message that additional efforts are needed to promote a rules-based international order – through both bilateral and regional cooperation. The expanding web of bilateral 'cyber agreements' such as those concluded between China and Australia or the US and China is one option. At the same time, state and non-state actors need to be conscious that, even in the absence of universal agreement on what laws apply to cyberspace and how, the international community has tools at its disposal to ensure that no malicious activity goes unpunished.

While the lawfulness of countermeasures under existing law is still under debate, the US, for instance, has already introduced cyber-related sanctions against entities and individuals in North Korea and Russia. The EU, too, is working on the Cyber Diplomacy Toolkit, which foresees the use of sanctions and other instruments against perpetrators, even though 'hacking back' on the basis of the Mutual Defence Clause or launch of a 'EUFOR CYBER' to assist partner countries are for the moment off the table. A big challenge for cyber diplomacy in the coming years will be to reinforce the existing 'volatile' consensus within multilateral organisations like the UN. This could be achieved, *inter alia*, through a more strategic deployment of existing instruments, in particular capacity-building programmes, in order to strengthen the efforts of organisations like the Council of Europe and mobilise partner countries.

The EU's cyber diplomacy, however, should not only be *reactive* by default. By throwing the full weight of its external action – trade, development, home affairs and even CSDP – behind cyber diplomacy, the EU can better enforce existing international laws (for example the Council of Europe Convention on Cybercrime) and ensure states' compliance with their international obligations (on the basis of the Mutual Legal Assistance or trade and investment agreements for instance).

Through capacity building programmes to fight cybercrime and strengthen cybersecurity, the EU contributes to building resilience in partner countries, denies safe havens for cyber criminals, and reduces the risks of potential conflict by increasing the threshold of what could be classified as an armed attack. Introducing an equivalent of conditionality in cyber-related projects and programmes – a form of 'cyber conditionality' – and denying assistance to countries who intentionally refuse to address malicious cyber operations originating from their territory or do not respect other norms of responsible state behaviour, could potentially be a powerful tool.

Additional efforts are also needed to strengthen the resilience of countries and societies *vis-à-vis* cyber threats. This is a task that cannot be achieved by states alone: it requires the engagement of a broader stakeholder community, including academics, civil society organisations, and the private sector. It has been proven by the development community that the societies most resilient to conflicts are those with a well-developed 'infrastructure for peace', whereby different groups can constructively interact with one another to address potential sources of tension. Building such infrastructure in cyberspace means investing in the resources, values, skills and interdependent systems through which the risks of conflict can be mitigated. This vision does not require a new convention, but rather a clear definition and division of responsibilities between the various groups of stakeholders.

Patryk Pawlak is the Brussels Executive Officer and is responsible for cyber-related issues at the EUISS.

 | QN-AK-17-023-2A-N | ISBN 978-92-9198-590-6 | ISSN 2315-1110 | doi:10.2815/975608