Unpacking the GGE's framework on responsible state behaviour: International law

GLOBAL PARTNERS DIGITAL
gp-digital.org

At the UN First Committee, two processes—the UN Group of Governmental Experts (GGE) and the Open-ended Working Group—are currently exploring the same question: responsible state behaviour in cyberspace. This term comes from a 2015 report by the previous GGE, which defines it according to a framework of four components: 1) norms, rules and principles; 2) confidence-building measures; 3) capacity-building; 4) the application of international law in cyberspace.

Understanding these components is crucial to engaging effectively at the GGE and OEWG. In this series, we'll be looking at each component in turn—looking at what they mean, how they have been defined, and their relevance to human rights. In this entry, we examine international law in cyberspace. This explainer was authored by Sheetal Kumar and Ian Barber at Global Partners Digital, with support from Eneken Tikk, from Cyber Policy Institute.

What is international law?

International law is commonly understood as a set of rules binding upon states, both in times of peace and times of war. It is usually considered synonymous to its main sources which include international conventions, international custom as evidence of a general practice accepted as law, and widely recognised general principles of law.[1]

In practice, understanding of international law is also shaped by the work of international lawyers and scholars—such as developing arguments regarding how they understand a particular legal obligation, or studying the emergence and development of customs in a given field.

International law consists of a number of branches including international human rights law (IHRL) and international humanitarian law (IHL). IHRL applies at all times and deals specifically with the obligations of states to respect, protect and fulfill human rights. IHL is applicable during armed conflict and seeks to limit the effects of war by protecting people who are not participating in hostilities, and by restricting the means and methods of warfare. When examined together, these branches of international law create a framework for how states should interact with one another, and respect or protect human rights and human life in varying circumstances.

International law and the relations between states in particular is underpinned by a number of key concepts:

- **State sovereignty**: This concept refers to the ability of a state to control domestic affairs within its territory without external interference. Under international law, states are generally prohibited from interfering in those domestic affairs (known as the principle of "non-intervention").
- **Use of force and armed attack**: International law generally prohibits the use of force by states. An armed attack is a type of use of force which crosses a certain threshold of severity. Instead of using force, states are expected to use alternative methods to address perceived or actual violations of international law (referred to as "peaceful settlement of disputes").
- **Self-defence**: This refers to an exception to the general prohibition on the use of force by states, where it is in response to an armed attack.

While it may be tempting to see international law as a finite and commonly understood set of rules and concepts, it should also be seen as dynamic and fluid, and a space of contestation, especially in a domain as new as cyberspace. Discussions relating to international law in cyberspace are evolving as existing legal texts, such as the main sources of international law, are interpreted for a new context, including by the international legal community. In addition, states continue to define how international law applies in cyberspace through their actions and statements. As explained below, human rights defenders have a role to play in this space as they can encourage states to support interpretations of international law that lend themselves towards responsible state behaviour and the upholding of international human rights obligations.

Application of international law in cyberspace

Discussions relating to whether and how international law applies in cyberspace have been around since the late 1990s.[2] It was around this time that states started discussing the matter in multilateral settings, particularly through the lens of international peace and security in the UN First Committee. The five Groups of Governmental Experts (GGE) established by the First Committee have been particularly important in fostering understanding among states around the application of international law in cyberspace.

Discussions at the first GGE in 2004 reportedly centred around the need for a new international legal framework of cyberspace.[3] The subsequent GGE, in 2010, while mentioning international law, focused more on certain measures, like confidence-building measures[4], and capacity building[5], which it said could support international peace and security.

It wasn't until 2013, when the third GGE stated that "international law, in particular the UN Charter, is applicable to the cyber-sphere", that there was explicit recognition and consensus on the matter. It also referred to the applicability of state sovereignty and human rights.

The fourth GGE (2015) reaffirmed this in their report, and went further, in identifying key concepts of international law applicable to cyberspace including state sovereignty, the settlement of disputes by peaceful means, and the principle of non-intervention. In addition, the 2015 GGE report included eleven voluntary norms[6] to guide states, some of which are derived from international law. This report was adopted by consensus by the UN General Assembly, which indicated strong support for this recognition by all UN member states. It seemed to indicate at least temporary agreement that before a new international legal instrument is discussed, states first needed to clarify how international law should be interpreted in cyberspace based on the existing international framework.

However, the following GGE was unable to reach consensus, reportedly because of the inability of states to agree on how international law applies in cyberspace. To help address this, a new GGE, established in 2018 alongside an Open-Ended Working Group (OEWG) working on the same issues, included a call for all member states of the UN to provide their views on the application of international law in cyberspace, including its key concepts mentioned above. Some of these key concepts were explicitly mentioned in the 2013 and 2015 GGE reports, while others were discussed in the subsequent GGE,[7] which failed to produce a consensus report. They've also been discussed in the OEWG and in member states annual submissions to the Secretary General.[8]

It is important to recognise that there are some real challenges in understanding how these concepts apply in cyberspace. For example, there are damaging cyberattacks that can be conducted by states, but it remains unclear whether these should be classified as "use of force" in the same way that a kinetic attack would be. And although a cyberattack may in certain circumstances be seen as a violation of the principle of non-intervention, it is not clear what kind of response would qualify as legitimate.

As such, greater clarification is needed from states on how they see the application of key concepts of international law in cyberspace. Over time, state practice and behaviour, which indicates how they interpret certain cyber operations by other states, will also help to clarify how international law applies in cyberspace. For example, if states develop a practice of reacting to large-scale DDOS attacks which targets information infrastructure, and therefore the delivery of services, by stating that they amount to "use of force" then this will, over time, shape common understanding of what the threshold is for "use of force" in cyberspace.

Some states, including France, the UK, Australia, the Netherlands, and the US, have issued public statements and/or position papers on how international law applies in cyberspace.[9] The Inter-American Juridical Committee (CJI) is currently undertaking a compilation of OAS member states perspectives on these questions. The public statements already issued show some evolving areas of agreement. For example, there seems to be consensus among those who have publicly stated their views that international law has been violated if a cyber operation from another state causes physical damage, which is referred to as a kinetic attack. Be that as it may, no state has as yet accused another of a "use of force" or an "armed attack" through cyber operations.

However, there are also areas of disagreement. For example, there isn't agreement on what would rise to a threshold of an "armed attack" and therefore legitimise the use of "self-defence". Other areas of disagreement include whether or not collective self-defence or countermeasures by states in response to a cyber operation would be acceptable.[10] State's annual national submissions to the UN Secretary General, as called for in the UN First Committee's annual resolution, illustrate this disagreement.[11]

Apart from disagreements on the applicability of key international law concepts, there is also a lack of consensus among states on whether certain branches of international law are applicable to cyberspace at all. This is particularly the case when it comes to international humanitarian law (IHL), governed by key instruments such as the Geneva Convention,[12] which regulates the conduct of states during armed conflict. This is due to claims that the application of IHL to cyberspace could legitimise the "militarisation" of cyberspace or the use of cyberspace for military purposes. This disagreement was reportedly one of the sticking points that led to the breakdown of the 2017 GGE.[13] Therefore, contestation as to what branches

(cont'd)

of international law apply in cyberspace, particularly IHL, and how they apply, continue to shape discussions related to international law in cyberspace.

Some states argue that clarifying state understandings of the application of international law in cyberspace—through public statements and publications—is not enough; and that a new instrument of international law is needed. This has also been suggested by key private actors, as well as some scholars.[14]

What are the links between human rights and the application of international law in cyberspace?

As already mentioned, international human rights law (IHRL) forms part of international law and should therefore be part of any discussion on how international law applies in cyberspace. While applicability of IHRL in cyberspace has been discussed and elaborated elsewhere, particularly in Human Rights Council (HRC) resolutions[15] on the promotion, protection and enjoyment of human rights on the internet, the OEWG and GGE discussions are likely to inform our understanding of how IHRL applies in cyberspace, particularly in the context of international peace and security.

Due to the evolving nature of the interpretation of international law, human rights defenders can play an important role in shaping how states view and abide by international law and their international human rights obligations in this context. They can do this in three main ways: by monitoring and holding to account state behaviour in cyberspace, which includes their international human rights law obligations; by supporting the interpretation and implementation of the 11 GGE norms in a human rights respecting manner; and by encouraging states to publish their interpretations of international law in a way that reinforce human rights obligations and human-centric interpretations of international law.

States have already stated their commitment to international human rights obligations in cyberspace. This is reflected in the GGE's 2015 report as it explicitly provides that "States must comply with their obligations under international law to respect and protect human rights and fundamental freedoms". Many have referred to international human rights law in their public statements regarding the application of international law in cyberspace, including by referring to relevant HRC resolutions.[16] These HRC resolutions already provide some guidance in interpreting state obligations to respect and protect human rights in cyberspace. Specifically, they reiterate that international human rights law applies to state use of ICTs and that people enjoy the same international human rights with respect to cyber-related activities as they would in a non-cyber context. States are therefore subject to international human rights law obligations and must protect individuals from abuse by third parties. Human rights defenders can continue to remind states of their internationally binding legal obligations to protect human rights and hold states to account for them.

In addition, the way states interpret how international law applies in cyberspace continues to evolve and requires further clarity. This clarity can be provided by states in a way which is informed by and references human rights. Human rights defenders can play a role here by providing guidance on concrete issues as the recommendations included in the GGE report are in parts deliberately ambiguous and require clarification. For example:

- **Due diligence**: Due diligence is linked to the principle of state sovereignty. When applied to cyber operations, this principle would oblige a state to not knowingly allow its territory or the ICT infrastructure under its control to be used for cyber operations that affect the rights of other states. Yet, certain interpretations of this principle note that the obligation only attaches when an action would produce "serious adverse consequences" for other states. While some states support this view, others consider due diligence as a purely aspirational principle that does not involve a specific binding legal obligation in cyberspace. However, the fact that cyber operations can harm and infringe upon the human rights of individuals in other states makes the principle of due diligence imperative from a human rights perspective. Although it might be practically difficult to prove the "knowledge" element of this principle, as states can plausibly deny having actual or constructive knowledge of such activities, this does not render the legal obligation moot. Human rights defenders can encourage states to support the binding nature of this principle and advocate for a preventative approach to potential violations.
- **Non-intervention**: The prohibition of intervention is often described as the "corollary to every state's right to sovereignty, territorial integrity and political independence".[17] It is widely accepted that this principle would be violated if a state used cyber operations to directly manipulate another country's election results or interfere with the ability to hold an election. While there is little clarity from states on whether disinformation campaigns would similarly violate this principle, the international human rights law framework does address this very issue with provisions for the right to free and fair elections, the right to freedom of expression and the right to privacy. Human rights defenders should therefore advocate for states to recognise the explicit links between these rights and the principle of non-intervention.

(cont'd)

- **Countermeasures:** In order to respond to the use of force, states have a right "to take measures consistent with international law and as recognised in the Charter".[18] This reference to "measures consistent with international law" doesn't address the issue of countermeasures in cyberspace but presumably includes them. Limitations which apply to the use of countermeasures are referenced in Article 50 of the International Law Commission's Draft Articles on State Responsibility as it stipulates that countermeasures may not involve the use of force nor include actions that affect fundamental human rights or violate peremptory norms.[19] "Fundamental human rights" are not clearly defined by the Draft Articles on State Responsibility, which provides human rights defenders with an opportunity to advocate for a broader reading of these rights. While other limitations on countermeasures, including the requirement of prior notice might not be feasible in a cyber context, limitations that protect human rights should continue to be respected by states.

The observation of the norms included in the 2015 GGE report also has an implication for international law, including human rights law.[20] A number of them are directly linked to the principle of due diligence, including norm 'c', which requires states to ensure that their territory is not used by "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". Observing these norms will therefore support states in abiding by their international law obligations. In addition, over time, repeated patterns of behaviour shaped by observation of the norms could lead to the crystallisation of these norms into customary international law, or their adoption into treaties. As such, while the 11 GGE norms adopted by states are referred to as "voluntary", their implementation in a way which respects human rights would not only have a positive impact on human rights, but could also shape international law in a rights-respecting manner.

End notes

1. Statute of the International Court of Justice (ICJ), Art 38
2. Michael N. Schmitt, "Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework", 37 COLUM. J. TRANSNAT'L L. 885, 886 (1999); Christopher C. Joyner & Catherine Lotrionte, "Information Warfare as International Coercion: Elements of a Legal Framework", 12 EUR. J. INT'L L. 825, 848 (2001); Wingfield TC (2000) "The law of information conflict: national security law in cyberspace". Aegis Research Corporation, Falls Church.
3. UN Doc A/58/373, 17 September 2003.
4. "Unpacking the GGE's framework on responsible state behaviour on cyberspace: Confidence-building measures", https://www.gp-digital.org/publication/unpacking-the-gges-framework-on-responsible-state-behaviour-capacity-building-2/
5. "Unpacking the GGE's framework on responsible state behaviour on cyberspace: Capacity building", https://www.gp-digital.org/publication/unpacking-the-gges-framework-on-responsible-state-behaviour-capacity-building/
6. Unpacking the GGE's framework on responsible state behaviour on cyberspace: Cybernorms", https://www.gp-digital.org/publication/unpacking-the-gges-framework-on-responsible-state-behaviour-cyber-norms/
7. UN Doc A/C.1/72/PV.19
8. Mika Kerttunen and Eneken Tikk, "Strategically normative. Norms and principles in national cybersecurity strategies" (EUISS, 2019) https://eucyberdirect.eu/content_research/a-normative-analysis-of-national-cybersecurity-strategies/ See also Annex 1 to 'Strategically normative' at: https://eucyberdirect.eu/content_research/1230/
9. Ministère des Armées, "Droit international applique aux opérations dans le cyberespace" ; United Kingdom Attorney General's Office, "Cyber and International Law in the 21st century" ; Australian Government Department of Foreign Affairs and Trade "2017 – Australia's position on the application of international law to state conduct in cyberspace", "2019 - Australia's position on the application of international law to state conduct in cyberspace"; Government of Netherlands Ministry of Foreign Affairs "Letter to the parliament on the international legal order in cyberspace"; US Department of Defense, "DOD General Counsel Remarks at U.S. Cyber Command Legal Conference".
10. Michael Schmitt, Just Security, "Estonia Speaks Out on Key Rules for Cyberspace"
11. Mika Kerttunen and Eneken Tikk, "Strategically normative. Norms and principles in national cybersecurity strategies" (EUISS, 2019) https://eucyberdirect.eu/content_research/a-normative-analysis-of-national-cybersecurity-strategies/ See also Annex 1 to 'Strategically normative' at: https://eucyberdirect.eu/content_research/1230/
12. Geneva Conventions of 1949 (I-IV) and their Additional Protocols
13. UN Doc A/C.1/72/PV.19
14. https://www.microsoft.com/en-us/cybersecurity/content-hub/a-digital-geneva-convention-to-protect-cyberspace; https://www.researchgate.net/publication/228222998_Why_States_Need_an_International_Law_for_Information_Operations; https://link.springer.com/article/10.1007/s13347-017-0271-5
15. UN Human Rights Council, The promotion, protection and enjoyment of human rights on the Internet: resolution / adopted by the Human Rights Council, A/HRC/32/L.20
16. UN General Assembly, Report of the Secretary-General A/68/156, p. 5; UN General Assembly, Report of the Secretary-General A/64/129, p.10; UN General Assembly, Report of the Secretary-General A/66/152, p. 3.
17. Oppenheim, Oppenheim's International Law, Vol 1: Peace, (1996) p. 428
18. UN GGE Report 2015 (A/70/174)
19. Articles on State Responsibility, Art 50.
20. UN GGE Report 2015 (A/70/174)