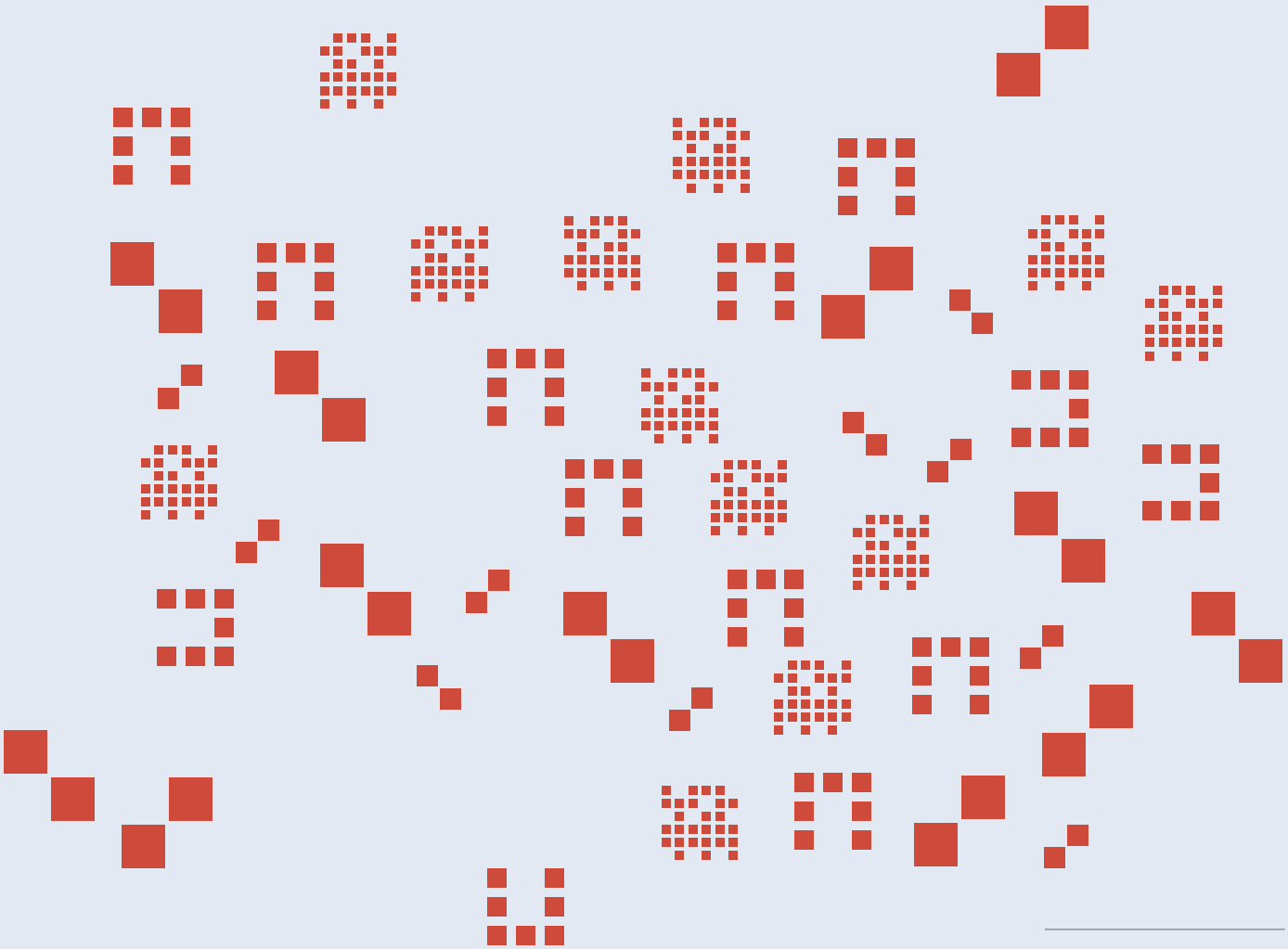
GLOBAL PARTNERS DIGITAL

Application of International Law in Cyberspace: Human Rights Assessment Guide



March 2023

Contents

Acknowledgments

This guide was authored by Ian Barber. We are grateful to Kubo Mačák and Talita Dias for their review and feedback.

Introduction

In the last few years, more states have started to provide their views on the applicability of international law—including in some cases international human rights law (IHRL)—in cyberspace.

This is a relatively new phenomenon. Even though the applicability of international law in cyberspace has long had broad consensus in the international community[1], it was uncommon to see official, detailed state positions on it. And even now, the total number of states providing such positions remains low.

From a human rights perspective, it's critical that more states provide their views on how international law applies in cyberspace[2]—particularly detailed, human-centric and human rights-promoting perspectives. This is because the use of information and communication technologies (ICTs) by states, including as a tool of foreign policy, can negatively impact human rights. For example, the use of ICTs by states may result in violations of the right to privacy, they may limit access to information or restrict individuals' right to freedom of expression. Cyber operations can influence or subvert a country's democratic processes and undermine individuals' right to free and fair elections. In the most severe cases, state-sponsored cyber operations may even pose risks to an individual's right to health or the right to life, particularly when they target the healthcare sector, as was the case during the COVID-19 pandemic.

As more positions have been developed, we've been able to see examples of both good and bad practice. How, then, can we encourage states to develop better positions?

About this guide

That's where this guide comes in. Its aim is to provide a clear framework for civil society and government actors to assess state positions on the application of international law in cyberspace. In doing so, they can effectively and constructively advocate for rights-respecting state positions.

The framework presented in this guide is broken down into eight separate topics which have particular consequences for human rights.

It was designed to examine and assess a variety of different outputs covering state positions on the application of international law in cyberspace. This includes published government reports, inputs, and commentary at international processes such as the GGE or OEWG, as well as individual statements from high-level government officials. It may also be used to assist states seeking to draft or update their own perspectives.

The guide

A state's position on the application of international law in cyberspace may take a number of forms. They set out how a particular state considers specific international rules, principles and bodies of law apply to the use of ICTs by states. After reviewing the positions of dozens of states,[3] this guide has identified some of the most common topics addressed which have particular consequences for human rights.

- Application of international law in cyberspace
- Respect for human rights and fundamental freedoms
- Sovereignty
- Non-intervention
- Due diligence
- Peaceful settlement of disputes
- Countermeasures
- Use of force

The topics are not listed in order of importance. Each topic is described to help the user understand what the links are between the topics and human rights. The links will be stronger in relation to some topics than others, but in many cases, its inclusion in state positions – if consistent with the requirements set out for each topic – will support the enjoyment of human rights or otherwise support human-centric considerations.

1. Application of international law in cyberspace

This refers to a state's acknowledgement of the application of international law in cyberspace, particularly the UN Charter, customary international law, international humanitarian law and international human rights law.[4] It is considered to be a baseline consideration. Most, if not all, states make clear that they consider international law to apply in cyberspace, but in the past, some had challenged the applicability of specific rules, principles or entire

bodies of law—most notably international humanitarian law (IHL). An important milestone in this regard was the 2021 GGE report, in which states expressly referred to IHL in the cyber context.[5] This has been widely interpreted as amounting to a consensus among states that IHL is applicable to cyber operations.[6] The view that IHL applies to, and therefore limits, cyber operations during armed conflict is also shared by the International Committee of the Red Cross, an organisation mandated by states to serve as the guardian of IHL.[7]

It is important that states acknowledge the application of international law in its entirety as it is essential to maintaining peace and stability in cyberspace. States should commit themselves to reaching a common understanding of how existing international law applies where there is disagreement. This is critical because, when examined together, international law and its various branches create an overlapping framework for how states should interact with one another, and respect or protect human rights in varying circumstances. It is therefore imperative that states do not attempt to challenge the application of one or more of these frameworks and their protective value.

What does a human rights-promoting and human-centric approach look like?

- A human rights-promoting and human-centric approach includes an explicit recognition of the application of international law in its entirety, including the UN Charter, customary international law, as well as various branches such as international human rights law and international humanitarian law.
- States should ideally make reference to applicable legal instruments beyond the UN Charter, including international human rights treaties and international humanitarian law conventions.
- State positions on the application of international law in cyberspace should not challenge the application of specific rules, principles or bodies of law. They should avoid, for example, language that suggests that the applicability of international humanitarian law in some way encourages the

militarisation of cyberspace or legitimises cyber conflict. In fact, as recognized in the 2021 GGE report, recalling IHL principles "by no means legitimises or encourages conflict".

- States should commit themselves to reaching a common understanding of how existing international law applies where there is disagreement.

What examples exist of good practice?

(Czech Republic): "...existing international law applies to cyberspace in its entirety. Indeed, existing international law provides us with all the necessary tools to prevent actual conflicts in cyber domain. The issue at stake is not a gap in existing law, but compliance with existing law and reaching a common understanding on how to apply the law to today's environment."

"In particular, the Czech Republic wishes to reiterate that international human rights law is applicable to cyberspace in its entirety."

"The Czech Republic recognizes that International humanitarian law (IHL) applies to cyber operations during armed conflicts, on the understanding that this neither encourages the militarization of cyberspace, nor legitimizes cyber warfare, just as IHL does not legitimize any other form of warfare".[8]

(Brazil): "Brazil firmly believes that in their use of information and communications technologies, States must comply with international law, including the United Nations Charter, international human rights law and international humanitarian law. The United Nations and other regional organizations have recognized that international law, and in particular the Charter of the United Nations, is applicable to States' ICT-related activity in cyberspace and is essential to maintaining peace and stability and promoting an open, secure, peaceful and accessible ICT environment. Hence, in current discussions, the question is no longer whether, but how international law applies to the use of ICTs by States".[9]

2. Respect for human rights and fundamental freedoms

This refers to a state's obligations under international human rights law to respect, protect and promote human rights. States assume these obligations by becoming parties to international treaties or insofar as they are binding under customary international law. The obligation to respect requires states to refrain from interfering with or restricting the enjoyment of human rights. The obligation to protect requires states to take specific steps or positive action to protect individuals and groups against human rights abuses by third parties. The obligation to fulfil, ensure or promote means that states must take positive action to facilitate the enjoyment of basic human rights.

Various UN GGE and OEWG reports, including the most recent iterations, reaffirm the commitment of states under international law to respect human rights and fundamental freedoms. It is important that states acknowledge their full spectrum of human rights obligations—that is, their obligations to respect, protect and promote human rights. This reinforces the binding nature of these obligations as they extend to both offline and online environments.[10]

What does a human rights-promoting and human-centric approach look like?

- A human rights-promoting and human-centric approach includes a clear recognition of a state's obligations under international human rights law to respect, protect and promote human rights. It should acknowledge that these obligations apply to both online and offline environments.
- States should ideally make reference to specific human rights most relevant in the digital context, including the right to privacy, freedom of expression and peaceful assembly, as well as to international human rights instruments more generally, particularly universal ones such as the Universal Declaration of Human Rights, the International Covenant on Civil and Political Rights and the International Covenant on Economic, Social and Cultural Rights.
- It would be beneficial to mention soft law instruments, including UN Human Rights Council resolutions, general comments

adopted by the UN Human Rights Committee and other UN treaty monitoring bodies, outputs of UN Special Procedures, and reports issued by Special Rapporteurs, all of which provide guidance in interpreting international human rights law and individual rights and corresponding state obligations that they give rise to.

What examples exist of good practice?

(Estonia): "All states bear an obligation to ensure and protect fundamental rights and freedoms both online as well as offline. In regards to state use of ICTs, states must comply with Human Rights obligations including those deriving from the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights.

Cybersecurity and human rights are complementary, mutually reinforcing and interdependent. Both need to be pursued together to effectively promote freedom and security. Cybersecurity laws, policies and practices must not be used as a pretext to silence human rights defenders and restrict human rights and fundamental freedoms in general.

The prevention, mitigation of as well as responses to cyber incidents should not violate human rights. This in particular includes the freedom of expression, the freedom to seek, receive and impart information, the freedom of peaceful assembly and association, and the right to privacy".[11]

(Netherlands): "States have a duty to respect and protect the human rights of every person within their jurisdiction. This implies not only a 'negative' duty - i.e. to refrain from acts in violation of human rights - but also a 'positive' duty to ensure that people can genuinely exercise their rights and defend themselves against violations by others. It is for instance not sufficient for the Dutch government to respect the privacy of Dutch citizens. It must also take measures to ensure that, for example, companies respect the privacy of their customers".[12]

3. Sovereignty

Sovereignty is a fundamental principle of international law which can be understood as a state's ability to exclusively govern all persons, property, and activities within its territory. It places a responsibility on states to respect the sovereignty of other states and not behave in ways that are contrary to their sovereign rights. The principle of sovereignty is closely related to other principles of international law including the prohibition of intervention. Various GGE reports affirm that state sovereignty and principles that flow from sovereignty apply to the use of ICTs by states and to their jurisdiction over ICT infrastructure within their territory.

There is some debate as to whether this principle operates as a standalone rule of international law which, if violated, would constitute an internationally wrongful act and engage the international responsibility of the offending state, which may result in consequences for the offending state provided that the relevant substantive and procedural conditions are met.[13] Among those states that have expressed their views on the application of international law in cyberspace, the vast majority accepted sovereignty as a standalone rule. However, the UK does not consider it as a standalone rule, but instead as a principle which should guide interactions between states.[14] According to this minority view, cyber operations cannot violate the victim state's sovereignty but only other rules or principles of international law, such as the principle of non-intervention. This approach arguably poses potential risks for human rights and security as it would enable states to undermine the sovereign powers and functions of other states, such as their governmental policies, without facing any international responsibility and ensuing consequences. This carries serious risks for human rights protection domestically and abroad insofar as they are part and parcel of a state's sovereign functions.

However, most states and many scholars agree that sovereignty is a binding rule of international law which may be violated by certain cyber operations, and there is a need to address and come to a consensus as to which types of behaviour would violate this rule. This

approach thus provides an additional limitation on the use of ICTs by states which may have negative impacts on other states. As this guide will show in the following sections, proving violations of other rules or principles of international law that amount to international wrongful acts, such as a prohibited intervention or an unlawful use of force, is both demanding and uncertain. Arguing that sovereignty is not a rule simply affords states the flexibility to act with less restraint while claiming to operate within the boundaries of international law.

What does a human rights-promoting and human-centric approach look like?

- A human rights-promoting and human-centric approach acknowledges sovereignty as both a fundamental principle and a rule of international law. There should be an explicit acknowledgement that the principle of sovereignty also constitutes a standalone rule of international law that can be violated by states through the use of ICTs and thereby give rise to state responsibility for an internationally wrongful act.
- States should recognise that state sovereignty is not absolute but may be limited by obligations such as those under international human rights law.
- Ideally, states should indicate specific instances or examples where they consider cyber operations to violate the sovereignty of another state.

What examples exist of good practice?

(Brazil): "State sovereignty is one of the founding principles of international law. (…) It is applicable as a standalone rule, including to the use of ICTs by States, and entails an independent obligation of "every State to respect the territorial sovereignty of others". Currently, there is neither broad state practice nor sufficient *opinio juris* to generate new customary international norm allowing for the violation of State sovereignty, including by means of ICTs.

Violations of State sovereignty by another State, including by means of ICTs, constitute an internationally wrongful act and entail the international responsibility of the State in violation".[15]

(Netherlands): "Firstly, sovereignty implies that states have exclusive jurisdiction over all persons, property and events within their territory, within the limits of their obligations under international law, such as those relating to diplomatic privileges and immunity, and those arising from human rights conventions".[16]

4. Non-intervention

The principle of non-intervention is a rule which prohibits intervention in the external or internal affairs of other states. This rule is binding on all states as it is considered to be a part of customary international law and a violation would constitute an internationally wrongful act.[17] GGE and OEWG reports have consistently recognised that the principle of non-intervention applies to the use of ICTs by states.

The International Court of Justice (ICJ) has outlined the elements of activity that would constitute a violation of the principle of non-intervention: (1) it must relate to matters that fall within its *domaine réservé*, which is understood as the state's choice of political, economic, social and cultural system and formulation of foreign policy; and (2) there must be coercion by the offending state.[18] However, the scope of *domaine réservé* is contested and there is no universally accepted definition of "coercion" under international law. Several approaches to coercion have emerged in the cyber context, including one that considers an act as coercive when it compels the victim state to take a particular course of action, or refrain from it, when it would otherwise not voluntarily do so; and a second approach that considers coercion as depriving the victim state of its ability to control or govern matters within its *domaine réservé*.[19] This second approach is broader than the first as it accepts the mere deprivation of the victim state's control over a protected matter, without actually or potentially compelling the state to change its behaviour.

This topic is important from a human rights and human-centric perspective as it limits the ability of states to launch cyber operations which may have a negative impact on individuals and the enjoyment of human rights in other states, or interfere with a state's ability to

otherwise respect, protect and promote those rights. States have increasingly provided their perspectives on how cyber operations, particularly those targeted at elections and democratic processes, critical infrastructure or the state's ability to respond to public health emergencies, may violate this principle. In doing so, they make clear that this prohibition applies in ways which may safeguard human rights, even if not explicitly mentioning the links between such acts and specific human rights, such as the right to free and fair elections or the right to health.

What does a human rights-promoting and human-centric approach look like?

- A human rights-promoting and human-centric approach acknowledges that the principle of non-intervention applies to the use of ICTs by states or state support to certain activities carried out by non-state actors. Cyber operations that breach this principle constitute an international wrongful act giving rise to state responsibility under international law.
- States should advance broad interpretation of this principle, including on what constitutes coercion and falls under its its *domaine réservé*.
- States should share their views on when they believe cyber operations may violate this principle, for example, when the scale and effects of a certain act of interference are similar to a prohibited intervention in non-cyber contexts. This should include specific instances or illustrative examples where the state considers that cyber operations could amount to prohibited interventions.
- Ideally, states should recognise the explicit links between the principle of non-intervention and the ability of states to respect, protect and promote human rights. For example, a prohibited interference in the form of election interference may have an impact on freedom of expression, free and fair elections, the right to privacy, and peaceful assembly.

What examples exist of good practice?

(New Zealand): "Examples of malicious cyber activity that might violate the non-intervention rule include: a cyber operation that deliberately manipulates the vote tally in an election or deprives a significant part of the electorate of the ability to vote; a prolonged and coordinated cyber disinformation operation that significantly undermines a state's public health efforts during a pandemic; and cyber activity deliberately causing significant damage to, or loss of functionality in, a state's critical infrastructure, including – for example – its healthcare system, financial system, or its electricity or telecommunications network".[20]

(Germany): "Generally, Germany is of the opinion that cyber measures may constitute a prohibited intervention under international law if they are comparable in scale and effect to coercion in non-cyber contexts. (…) Germany generally agrees with the opinion that malicious cyber activities targeting foreign elections may – either individually or as part of a wider campaign involving cyber and non-cyber-related tactics – constitute a wrongful intervention. For example, it is conceivable that a State, by spreading disinformation via the internet, may deliberately incite violent political upheaval, riots and/or civil strife in a foreign country, thereby significantly impeding the orderly conduct of an election and the casting of ballots. Such activities may be comparable in scale and effect to the support of insurgents and may hence be akin to coercion in the above-mentioned sense. A detailed assessment of the individual case would be necessary.

Also, the disabling of election infrastructure and technology such as electronic ballots, etc. by malicious cyber activities may constitute a prohibited intervention, in particular if this compromises or even prevents the holding of an election, or if the results of an election are thereby substantially modified.

Furthermore, beyond the mentioned examples, cyber activities targeting elections may be comparable in scale and effect to coercion if they aim at and result in a substantive disturbance or even permanent change of the political system of the targeted State, i.e. by significantly eroding public trust in a State's political organs and processes, by seriously impeding important State organs in the fulfilment of their functions or by dissuading significant groups of citizens from voting, thereby undermining the meaningfulness of an election".[21]

5. Due Diligence

Due diligence primarily refers to a state's obligation to not knowingly allow its territory to be used for acts contrary to the rights of other states.[22] When applied to cyber operations, due diligence would oblige a state to not knowingly allow its territory or the ICT infrastructure under its control to be used for cyber operations that contravene the rights of other states. It has been referenced, perhaps indirectly, in the 2015 UN GGE report's conclusion 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". However, states have not reached consensus on whether due diligence is a general principle of international law, a binding obligation or the standards that are required to comply with a potential obligation.

A very limited number of states consider due diligence to be a purely aspirational principle, such as Israel, the UK and Argentina, whereas most states, including Australia, Czech Republic, Estonia, Finland, France, Germany, Italy, Japan, the Netherlands, South Korea, Sweden and others recognise it as a customary obligation with binding force.[23] This latter approach to due diligence is more favourable from a human rights and human-centric perspective as cyber operations are particularly well-suited to causing harm or posing risks to individual human rights in other states, and are increasingly conducted by non-state actors. Compliance with this binding obligation is likely to limit at least some forms of harmful cyber activities which impact other states and the human rights of individuals in those states, as well as the rights of individuals within a particular state.

What does a human rights-promoting and human-centric approach look like?

- States should acknowledge that the concept of due diligence is binding - whether as a principle, rule or standard of conduct – and gives rise to binding obligations under international law which apply in cyberspace and require a state to exercise its best efforts to prevent, stop of redress certain harms, including

the obligation to not knowingly allow its territory to be used for acts that are contrary to the rights of other states.

- States should provide further information as to the exact measures of due diligence states must put in place to meet the requisite standard of due diligence and thus comply with their respective obligations to prevent, stop or redress harm.

What examples exist of good practice?

(France): "In compliance with the due diligence requirement, it ensures that its territory is not used for internationally wrongful acts using ICTs. This is a customary obligation for States, which must (i) use cyberspace in compliance with international law, and in particular not use proxies to commit acts which, using ICTs, infringe the rights of other States, and (ii) ensure that their territory is not used for such purposes, including by non-state actors".[24]

(Estonia): "The due diligence obligation of a state not to knowingly allow its territory to be used for acts that adversely affect the rights of other states has its legal basis in existing international law and applies as such in cyberspace."

"In addition, due diligence is related to taking action by applying all lawful and feasible measures in order to halt an ongoing malicious cyber operation. States should strive to develop means to offer support, when requested by the injured state, to identify or attribute malicious cyber operations. These actions could for example include warning, cooperating and sharing relevant data pertaining to an incident, investigating the incident and prosecuting the perpetrators, assisting the victim state(s) or accepting assistance".[25]

6. Peaceful Settlement of Disputes

The peaceful settlement of disputes is a fundamental principle of international law. Article 2(3) of the UN Charter provides that "All Members shall settle their international disputes by peaceful means in such a manner that international peace and security, and justice, are not endangered". Article 33 of the UN Charter further provides that states are required to seek the settlement of disputes by peaceful means such as negotiation, enquiry, mediation, conciliation,

arbitration, judicial settlement, resort to regional agencies or arrangements, or other peaceful means of their choice. Article 37(1) of the UN Charter stipulates that states must refer a dispute to the UN Security Council if those peaceful efforts to resolve it fail.

Various states and UN GEE/OEWG reports have recognised the applicability of this obligation to cyber activities. This topic is important from a human rights and human-centric perspective as it seeks to resolve disputes, including disputes which relate to the cyber context, peacefully without resulting in the threat or use of force. This can help prevent escalation and reduce risks to human rights or human life associated with such escalation.

What does a human rights-promoting and human-centric approach look like?

- States should explicitly recognise that it is an obligation for states to settle their international disputes by peaceful means, including disputes which relate to the cyber context.
- States should commit themselves to resolving disputes peacefully as laid out in Articles 2(3) and 33 of the UN Charter, as well as to referring disputes to the UN Security Council should other peaceful means of dispute resolution fail to resolve the issue as required under Article 37(1). They should also consider which means of peaceful dispute settlement are more appropriate to resolve cyber disputes.

What examples exist of good practice?

(Japan): "Any international disputes involving cyber operations must be settled through peaceful means pursuant to Article 2(3) of the UN Charter. In addition, pursuant to Article 33 of the UN Charter, the parties to any dispute involving cyber operations, the continuance of which is likely to endanger the maintenance of international peace and security, must first of all seek a solution by negotiation, enquiry, mediation, conciliation, arbitration, judicial settlement, resort to regional agencies or arrangements, or other peaceful means of their own choice. In order to ensure the peaceful settlement of disputes, the powers of the Security Council based on Chapters VI and VII of the UN Charter and the functions of the other UN

organs, including ICJ based on Chapter XIV of the UN Charter and the Statute of the International Court of Justice should be used in dispute stemming from cyber operations".[26]

7. Countermeasures

Countermeasures are acts or omissions by states that would normally be considered a violation of an obligation under international law, but are permissible if taken in response to a previous internationally wrongful act committed by another state, provided that the relevant substantive and procedural conditions are met.[27] Countermeasures are distinct from acts taken in response to undesirable conduct by another state that are technically legal, albeit unfriendly in nature (also referred to as "retorsions"). The UN GGE reports do not make explicit reference to countermeasures, but the 2021 report provides that "an affected State's response to malicious ICT activity attributable to another State should be in accordance with its obligations under the Charter of the United Nations and other international law, including those relating to ... internationally wrongful acts".[28]

A state's ability to respond to an internationally wrongful act with countermeasures is constrained by substantive and procedural requirements applicable under customary rules of state responsibility. These are arguably reflected in specific provisions of the International Law Commission's Articles on the "Responsibility of States for Internationally Wrongful Acts".[29] Article 49 provides that countermeasures may only be undertaken to induce the responsible state's compliance with its obligations and Article 50 stipulates that countermeasures cannot involve the threat or use of force, violate fundamental human rights or peremptory norms of international law.[30] These conditions and limitations are widely considered to reflect customary international law, and are critical from a human rights perspective as they restrict the ability of states to respond to internationally wrongful acts in ways that either risk escalation or pose risks to human rights.

What does a human rights-promoting and human-centric approach look like?

- States should explicitly recognise that states have a right to take countermeasures, but only provided that the applicable conditions are met – in particular, they may only be taken in response to behaviour (such as malicious ICT activity) attributed to another state that constitutes an internationally wrongful act.
- In particular, states should acknowledge that countermeasures, whether cyber in nature or not, must only be adopted to stop an ongoing violation and bring about compliance with international obligations. They must not be undertaken with the purpose of antagonising or punishing the violating state or escalating tensions.
- States should acknowledge that countermeasures must be proportionate, and may not involve the threat or use of force, violate fundamental human rights or peremptory norms of general international law. [31]

What examples exist of good practice?

(Switzerland): "In cases where an act violates international law and can be legally attributed to a state, the injured state(s) may also take countermeasures in the form of reprisals, provided that the applicable rules governing state responsibility are observed. Although reprisals are contrary to international law, they are justified in response to a prior breach of international law. However, such a countermeasure must not violate certain fundamental substantive obligations such as the prohibition on the use of force, fundamental human rights, most norms of international humanitarian law, peremptory norms (*jus cogens)* and the obligation to respect diplomatic and consular inviolability. Military force, i.e. measures leading to loss of life and limb, are therefore prohibited".[32]

8. Use of Force

The prohibition on the threat or use of force is a fundamental rule of international law and is set out in Article 2(4) of the UN Charter. The prohibition on the use of force has two exceptions, including in the case of self-defence against an armed attack and when authorised by the United Nations Security Council. International law does explicitly define what amounts to a prohibited "use of force". But the drafting history of the United Charter and case law from the ICJ indicate that the prohibition applies to all uses of military force regardless of what type or weapon or means are employed,[33] and thus extends to the use of ICTs.

This is further supported by several UN GGE reports, including the 2021 report, which provides that "In their use of ICTs, and as per the Charter of the United Nations, States shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any State or in any other manner inconsistent with the purpose of the United Nations". There is, however, a lack of consensus as to what type of cyber activity reaches the threshold of a prohibited use of force. Some states argue that the threshold for the use of force in a cyber context should be based on whether the cyber operation has a similar effect to those which would result from the use of conventional weapons, but others provide more nuanced criteria in making their assessments.

Some states, such as the United States, consider a violation of the use of force to be the same as an "armed attack". Article 51 of the UN Charter provides that states may resort to self-defence (which includes the use of force) in response to an "armed attack". This minority view would enable a victim state to respond to every violation of the prohibition on the threat or use of force with force themselves. Most states disagree with this view and differentiate between the use of force and an armed attack - providing a higher threshold for armed attack.[34] This is beneficial as a violation of the use of force constitutes an internationally wrongful act, but the victim state would only be able to respond with non-violent countermeasures. Therefore, distinguishing between the use of force

and armed attack provides more limitations on when states may resort to the use of force themselves.

Upholding the prohibition on the use of force and differentiating what amounts to a "use of force" from an armed attack are important from a human rights and human-centric perspective. This is true insofar as they further deter cyber operations which may have a negative impact on individuals' safety and well-being. While not often framed as a human rights issue, the protective value of this prohibition may have a positive impact on individuals' human rights, including the right to life, safety and security. For example, when cyber operations involving the use of force are used to target critical infrastructure or disrupt essential services they might infringe upon a range of human rights.

What does a human rights-promoting and human-centric approach look like?

- States should explicitly acknowledge that the prohibition on the threat or use of force applies in cyberspace, and distinguish between thresholds that apply to the use of force and those that constitute an armed attack.
- States should share their views on how to evaluate whether the threshold of the use of force has been crossed, as well as for an armed attack, and set out what specific criteria are used for these evaluations.
- Ideally, human rights should form part of these criteria and involve some consideration on how activities may affect the enjoyment of human rights.

What examples exist of good practice?

(Australia): "In determining whether a cyber activity constitutes a use of force, States should consider whether the activity's scale and effects are comparable to traditional kinetic operations that rise to the level of use of force under international law. This involves a consideration of the intended or reasonably expected direct and indirect consequences of the cyber activity, including for example whether the activity could reasonably be expected to cause serious or

extensive ('scale') damage or destruction ('effects') in the form of injury or death to persons, or damage or destruction (including to their function) to objects or critical infrastructure".[35]

(France): "A cyber operation carried out by one State against another State violates the prohibition of the use of force if its effects are similar to those that result from the use of conventional weapons. … However, not every use of force is an armed attack within the meaning of Article 51 of the United Nations Charter, especially if its effects are limited or reversible or do not attain a certain level of gravity. (…)

"France reaffirms that a cyberattack may constitute an armed attack within the meaning of Article 51 of the United Nations Charter, if it is of a scale and severity comparable to those resulting from the use of physical force. In the light of these criteria, the question of whether a cyberattack constitutes armed aggression will be examined on a case-by-case basis having regard to the specific circumstances. A cyberattack could be categorised as an armed attack if it caused substantial loss of life or considerable physical or economic damage. That would be the case of an operation in cyberspace that caused a failure of critical infrastructure with significant consequences or consequences liable to paralyse whole swathes of the country's activity, trigger technological or ecological disasters and claim numerous victims. In such an event, the effects of the operation would be similar to those that would result from the use of conventional weapons".[36]

Endnotes

[1] There is near universal consensus that international law applies in cyberspace. This is evident from the outputs of several processes established by the First Committee of the United Nations General Assembly— - the Groups of Governmental Experts (GGE) and the Open-Ended Working Groups (OEWG). States are simultaneously providing their own interpretations of the application of international law in cyberspace. These efforts have been complemented by those undertaken by legal scholars, who disseminate their views and contribute to academic initiatives such as the Tallinn Manuals and the Oxford Process on International Law Protections in Cyberspace.

[2] This guide does not consider "cyberspace" as a new domain of state activity that requires domain-specific state practice and *opinio juris*. It uses "the application of international law in cyberspace" and "the use of ICTs by state" interchangeably.

[3] See, Cyber Law Toolkit, National Positions, https://cyberlaw.ccdcoe.org/wiki/Category:National_position

[4] International law consists of a number of general rules and principles of international law, as well as specific branches such as international human rights law and international humanitarian law. International human rights law applies at all times and deals specifically with the obligations of states to respect, protect and fulfil human rights. International humanitarian law is only 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.

[5] UNGA, Report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security, UN Doc. A/76/135, 14 July 2021, p. 18, para. 71(f).

[6] Michael Schmitt, "The Sixth United Nations GGE and International Law in Cyberspace", Just Security (2021); and Adina Ponta, "Responsible State Behavior in Cyberspace: Two New Reports from Parallel UN Processes", ASIL Insight, 30 July 2021.

[7] ICRC, International Humanitarian Law and the Challenges of Contemporary Armed Conflicts, ICRC Report, (2015) p. 40.

[8] Czech Republic, Statement by Mr. Richard Kadlčák at the 2nd substantive session of the Open-ended Working Group on developments in the field of information and telecommunications in the context of international security of

the First Committee of the General Assembly of the United Nations, (2020), https://www.nukib.cz/download/publications_en/CZ%20Statement%20-%20OEWG%20-%20International%20Law%2011.02.2020.pdf

[9] Official compendium of voluntary national contributions on the subject of how international law applies to the use of information and communications technologies by States submitted by participating governmental experts in the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security established pursuant to General Assembly resolution, (13 July 2021), A/76/136, pp 17-23.

[10] UN Human Rights Council, Resolution "The promotion, protection and enjoyment of human rights on the Internet", (2021), UN Doc. A/HRC/RES/32/13.

[11] Official compendium of voluntary national contributions on the subject of how international law applies to the use of information and communications technologies by States submitted by participating governmental experts in the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security established pursuant to General Assembly resolution, (13 July 2021), A/76/136, p 27.

[12] Ibid, pp 60-61.

[13] An internationally wrongful act includes an action or omission by a state which is attributable to that state and constitutes a breach of an international obligation. States may respond to internationally wrongful acts in the form of countermeasures provided that the relevant substantive and procedural conditions are met.

[14] For example, Jeremy Wright, 'Cyber and International Law in the 21st Century' (23 May 2018) (stating that he was 'not persuaded that we can currently extrapolate from that general principle a specific rule or additional prohibition for cyber activity beyond that of a prohibited intervention. The UK government's position is therefore that there is no such rule as a matter of current international law').

[15] Official compendium of voluntary national contributions on the subject of how international law applies to the use of information and communications technologies by States submitted by participating governmental experts in the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security established pursuant to General Assembly resolution, (13 July 2021), A/76/136, p 18.

[16] Ibid, p 56.

[17] The rule of non-intervention is derived from the concept of sovereignty, and could be the basis of finding a violation of an international legal obligation in the

event that sovereignty is not considered a rule of international law which can be violated through the use of ICTs by states.

[18] International Court of Justice (ICJ), Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America), Merits, Judgement 27 June 1986, I.C.J. Reports 1986, para. 205.

[19] Cyber Law Toolkit (Prohibition of Intervention) https://cyberlaw.ccdcoe.org/wiki/Prohibition_of_intervention

[20] New Zealand, The Application of International Law to State Activity in Cyberspace, (2020), https://dpmc.govt.nz/sites/default/files/2020-12/The%20Application%20of%20International%20Law%20to%20State%20Activity%20in%20Cyberspace.pdf

[21] Germany, "On the Application of International Law in Cyberspace", Position Paper, to be annexed to the Report of the 2021 UN GGE on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security (March 2021), pp 4-5.

[22] Corfu Channel Case (UK v Albania), Merits, Judgment of 9 April 1949, ICJ Reports 1949, 4, p 22.

[23] Schmitt, supra, note 7. (noting that Israel took the surprising position, alongside Argentina, that no rule of due diligence applies in cyberspace. This should be contrasted with a large group of states who take the opposite perspective, but ultimately most states have not taken a firm position).

[24] Ministère des Armées, Droit International Appliqué aux Opérations dans le Cyberspace, (2019), https://www.justsecurity.org/wp-content/uploads/2019/09/droit-internat-appliqué-aux-opérations-cyberespace-france.pdf

[25] Official compendium of voluntary national contributions on the subject of how international law applies to the use of information and communications technologies by States submitted by participating governmental experts in the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security established pursuant to General Assembly resolution, (13 July 2021), A/76/136, pp 25-26.

[26] Official compendium of voluntary national contributions on the subject of how international law applies to the use of information and communications technologies by States submitted by participating governmental experts in the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security established pursuant to General Assembly resolution, (13 July 2021), A/76/136, p 49.

[27] Nicaragua judgement (supra note 19) para. 249.

[28] GGE Report 2021, (supra note 6) para 25.
[29] International Law Commision, Responsibility of States for Internationally Wrongful Acts, 2001.
[30] Responsibility of States for Internationally Wrongful Acts, Yearbook of the International Law Commission, Vol. II, Part 2, A/56/10/ (2001), Article 50.
[31] Peremptory norms, or jus cogens norms, are fundamental international legal norms that may not be derogated from under any circumstances. These norms include the prohibitions of slavery, genocide, aggression, and torture; the principle of non-refoulement; and the basic rules of international humanitarian law.
[32] Official compendium of voluntary national contributions on the subject of how international law applies to the use of information and communications technologies by States submitted by participating governmental experts in the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security established pursuant to General Assembly resolution, (13 July 2021), A/76/136, p 90.
[33] Legality of the Threat or Use of Nuclear Weapons in Armed Conflict - ICJ Advisory Opinion of 8 July 1996, para 39.
[34] Nicaragua judgement (supra note 19) para. 191.
[35] Official compendium of voluntary national contributions on the subject of how international law applies to the use of information and communications technologies by States submitted by participating governmental experts in the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security established pursuant to General Assembly resolution, (13 July 2021), A/76/136, pp 5-6.
[36] Ministère des Armées, Droit International Appliqué aux Opérations dans le Cyberspace, (2019), https://www.justsecurity.org/wp-content/uploads/2019/09/droit-internat-appliqué-aux-opérations-cyberespace-france.pdf