Estonian contribution on the subject of how international law applies to the use of information and communications technologies by states, to be annexed to the report of the Group of Governmental Experts on Advancing responsible state behaviour in cyberspace (2019-21)

Estonia welcomes the opportunity to submit its national contribution on the subject of how international law applies to the use of information and communications technologies (ICTs) by states as an annex to the report of the UN Group of Governmental Experts, as requested by UN General Assembly Resolution 73/266.

Estonia reiterates that existing international law applies in cyberspace. The rights and obligations set out in international law, including the UN Charter in its entirety, customary international law, international humanitarian and human rights law, apply to the use of ICTs by states. This means that international law applies to relations between states in cyberspace as it does in conventional domains of state interaction. To promote peace and stability in cyberspace and prevent conflict, it is necessary to have clear rules of responsible state behaviour in place.

Existing international law provides a solid normative framework for state actions, regardless of the means or the environment for these actions. The applicability of international law in cyberspace has been affirmed by the UN General Assembly endorsements of the 2013 and 2015 UN Group of Governmental Experts (GGE) consensus reports[1] and reaffirmed by the OEWG consensus report.[2] The current rules are technologically neutral and underline that state behaviour and the deployment of new transformative technologies do not change the applicability of international law.

States should strive to deepen a common understanding of how international law applies in cyberspace, alongside its possible implications and legal consequences. It is important to analyse how existing rules apply before discussing the need for any new agreement. Estonia sees notions for a new legally binding instrument as premature. From our perspective, current legal measures are sufficient to offer guidance on responsible state behaviour in cyberspace.

The 2013 and 2015 GGEs made substantive progress in terms of discussions on relevant legal rules and principles. In order to maintain peace and stability and promote an open, secure, peaceful and accessible cyberspace, we reiterate the following non-exhaustive elements: international law, including the UN Charter in its entirety, applies to state conduct in cyberspace, noting the principles of humanity, necessity, proportionality and distinction as well as respect for human rights and fundamental freedoms; states must meet their international obligations regarding internationally wrongful acts attributable to them under international law; states must not use proxies to commit internationally wrongful

[1] A/68/98*, adopted by UN General Assembly resolution A/RES/68/243; A/70/174, adopted by UN General Assembly resolution A/RES/70/237
[2] A/75/816, adopted by UN General Assembly Decision A/DEC/75/564

acts using ICTs, and should seek to ensure that their territory is not used by non-state actors to commit such acts; states must observe, among other principles of international law, sovereignty, sovereign equality, the settlement of disputes by peaceful means and non-intervention in the internal affairs of other States; the inherent right of States to take measures consistent with international law and as recognized in the Charter.

Alongside international law, voluntary, non-binding norms of responsible state behaviour can help prevent conflict in the ICT environment, reduce risks to international peace, security and stability and provide essential guidance for responsible state behaviour in cyberspace. Estonia underlines the importance of adhering to the set of voluntary non-binding norms reaffirmed in the UN General Assembly resolution 70/237. Together with confidence-building measures and capacity building measures, international law and norms constitute the framework for responsible state behaviour in cyberspace. We highlight that norms do not replace or alter States' obligations or rights under international law.

The paper first provides an overview of state obligations, followed by our position on state responsibility and attribution, and concludes with possible response options.

I. Obligations of states

Respect for sovereignty

Sovereignty as a fundamental principle of international law applies in cyberspace.

The 2013 and 2015 GGE consensus reports underscore that sovereignty and the international norms and principles that flow from it apply to state conduct of ICT-related activities. In addition, the 2013 GGE emphasised the importance of international law, the Charter of the UN and the principle of sovereignty as the basis for the use of ICTs by states.

States have territorial sovereignty over the ICT infrastructure and persons engaged in cyber activities on their territory. However, states' right to exercise sovereignty on their territory is not unlimited; states must respect international law, including human rights obligations. States also bear the responsibility to comply with legal obligations flowing from sovereignty — for example, the responsibility not to breach the sovereignty of other states and to take reasonable efforts to ensure that their territory is not used to adversely affect the rights of other states. The principle of sovereignty is also closely linked with the principle of non-intervention and the principles of the prohibition of the threat or use of force.

The violation of sovereignty through cyber means can breach international law, and therefore may give the victim state the right to take measures, including countermeasures. Views on what constitutes a breach of sovereignty in cyberspace differ. Malicious cyber operations can be complex, cross several

jurisdictions and may not always produce physical effects on targeted infrastructure.

Non-intervention

The principle of non-intervention is a well-established rule of international law, which flows from the principle of sovereignty, and applies to state conduct in cyberspace.

If an operation attributable to another state affects a state's internal or external affairs in such a manner that it coerces a state to take a course of action it would not voluntarily seek, it would constitute a prohibited intervention.

When discussing if a cyber operation constitutes an unlawful intervention into the external or internal affairs of another state, the element of coercion is a key factor. The possibility for a cyber operation to constitute an unlawful intervention in the functions that form a part of a state's *domaine réservé* has found acceptance among states, including Estonia, especially regarding the rights and obligations deriving from the principle of state sovereignty. States' *domaine réservé* according to the ICJ includes the "choice of a political, economic, social, and cultural system, and the formulation of foreign policy."[3] Stemming from that, cyber operations that aim to force another nation to act in an involuntary manner or to refrain from acting in a certain manner, and target the other nation's *domaine réservé* (e.g. national democratic processes such as elections, or military, security or critical infrastructure systems) could constitute such an intervention.

Prohibition of the use of force

States must refrain in their international relations from carrying out cyber operations which, based on their scale and effect, would constitute a threat or use of force against the territorial integrity or a political independence of any state, or in any other manner inconsistent with the purposes of the UN.

While taking measures in cyberspace, states must comply with the obligations and constraints enshrined in international law, including the UN Charter and customary international law. The threat or use of force in international relations is prohibited; however, the UN Charter foresees concrete situations where it could be allowed (in response to an armed attack, as self-defence or in accordance with chapter VII of the UN Charter).

The prohibition of the threat or use of force in cyberspace was also acknowledged and highlighted in the 2015 GGE report, endorsed by the UN General Assembly. Notably, the report states that "in considering the application of international law to State use of ICTs, the GGE identified as of central importance the commitments of States to the following principles of the Charter and other international law [...] refraining in their international relations from the

[3] Nicaragua case: www.icj-cij.org/files/case-related/70/070-19860627-JUD-01-00-EN.pdf

threat or use of force against the territorial integrity or political independence of any State [...]."[4]

A cyber operation that targets critical infrastructure and results in serious damage, injury or death, or a threat of such an operation, would be an example of use of force.

Due diligence

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.

The due diligence obligation derives from the principle of sovereignty. A state has the exclusive right to control activities within its territory. At the same time, this means that it is also obliged to act when its territory is used in a manner that adversely affects the rights of other states.

Without this obligation, international law would leave injured states defenceless in the face of malicious cyber activity that emanates from other states' territories. This is particularly relevant when state responsibility cannot be established. Therefore, states have to make reasonable efforts to ensure that their territory is not used to adversely affect the rights of other states. Such reasonable efforts are relative to national capacity as well as the availability of and access to information. Meeting this expectation encompasses taking all feasible measures in order to end the ongoing malicious cyber activity.

Estonia is at the position that the obligation of due diligence requires consideration of the technical, political and legal capacities of a state. 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. The necessary measures depend on the incident and are applied on a case-by-case basis.

International humanitarian law

If a situation amounts to an armed conflict and cyber operations are carried out during that conflict, international humanitarian law applies to these cyber operations as it does to all operations with a nexus to armed conflict in general.

[4] A/70/174, adopted by UN General Assembly resolution A/RES/70/237

Estonia believes that international humanitarian law sets boundaries for states' activities in conflict, protecting civilian persons and infrastructure, and acting as a constraint, not a facilitator of conflict.

In our view, international humanitarian law provides the necessary rules constraining states' conduct in conflict that also extend to cyber operations. Its applicability does not lead to the militarisation of cyberspace.

Armed conflicts today and in the future may involve offensive cyber capabilities. Therefore, it is vital that the use of such capabilities would be subject to obligations deriving from international humanitarian law, including taking into account such considerations as humanity, necessity, proportionality and distinction.

International human rights law

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.

As a founding member of Freedom Online Coalition (FOC) Estonia nationally and internationally supports policies and practices that promote the protection of human rights and fundamental freedoms online.[5]

Public authorities have a duty to respect and protect the freedom of expression and the freedom to seek, receive and impart information. Estonia is a proponent of transparency in government processes — transparency is essential in order for citizens to be able to trust the e-services provided to them. In addition, the development of e-government solutions in the public sector has to go hand in hand with safeguarding the privacy of citizens and the security of their data.

[5] Freedom Online Coalition statement on the Human Rights Impact of Cybersecurity Laws, Practices and Policies (2020): https://freedomonlinecoalition.com/wp-content/uploads/2020/02/FOC-Statement-on-Human-Rights-and-Cyber-Security-07.02.pdf

II. State responsibility and attribution

State responsibility

The law of state responsibility is a cornerstone for responsible state behaviour in cyberspace when it comes to assessing the unlawfulness of cyber operations below the threshold of use of force.

The law of state responsibility includes key principles that govern when and how a state is held responsible for cyber operations that constitute a breach of international obligation, by either an act or an omission. A cyber operation can constitute an internationally wrongful act if it is attributable under international law and it constitutes a breach of international obligation under the law of state responsibility. States must comply with customary international law mirrored in the Articles for Responsibility of States for Internationally Wrongful Acts.

States are responsible for their activities in cyberspace. States are accountable for their internationally wrongful cyber operations just as they would be responsible for any other activity according to international treaties or customary international law. State responsibility applies regardless of whether such acts are carried out by a state or non-state actors instructed, directed or controlled by a state.

States cannot waive their responsibility by carrying out malicious cyber operations via non-state actors and proxies. For example, if a hacker group launches cyber operations which have been tailored according to instructions from a state, or the cyber operations are directed or controlled by that state, state responsibility can be established.

Attribution

A cyber operation is deemed an internationally wrongful act when it is attributable to a state under international law and involves a breach of an international obligation of the state.

Attribution remains a national political decision based on technical and legal considerations regarding a certain cyber incident or operation. Attribution will be conducted on a case-by-case basis, and various sources as well as the wider political, security and economic context can be considered.

According to Article 2(a) of ARSIWA, an internationally wrongful act of a state has taken place when the conduct consisting of an action or omission is attributable to a state and the action or omission is wrongful under international law. Attribution allows establishing if a malicious cyber operation is linked with a state in order to invoke the responsibility of that state.

A state as a subject of international law can exercise its rights and obligations through its organs and in some instances by natural and legal persons. The attribution of an internationally wrongful act, including an internationally wrongful cyber operation, requires careful assessment of whether and how

malicious activity conducted by a person, a group of persons or legal persons can be considered as the act of a state. In principle, both acts and omissions are attributable to states.

Attribution is closely related to the availability of information of the malicious cyber operation. Following the various necessary assessments, public statements on attribution can be made, with the aim of increasing accountability in cyberspace and emphasising the importance of adhering to international law obligations and norms of responsible state behaviour.

III. State's response

In order to enforce state responsibility, states maintain all rights to respond to malicious cyber operations in accordance with international law. If a cyber operation is unfriendly or violates international law obligations, injured states have the right to take measures such as retorsions, countermeasures or, in case of an armed attack, the right to self-defence. These measures can be either individual or collective. The main aim of reactive measures in response to a malicious cyber operation is to ensure responsible state behaviour in cyberspace and the peaceful use of ICTs.

Peaceful settlement of disputes

It is an obligation for states to settle their international disputes that endanger international peace and security by peaceful means.

As outlined in the UN Charter, possible solutions to settle disputes between states include negotiation, enquiry, mediation, conciliation, arbitration, judicial settlement, resort to regional agencies or arrangements, and other internationally lawful action.

In accordance with the UN Charter Chapter VI, the UN Security Council may also call upon the parties, when it deems necessary, to settle their dispute by such peaceful means. In specific cases with respect to cyber activities endangering international peace and security, the other powers and responsibilities of the UN Security Council outlined in the UN Charter may be exercised in order to maintain and restore international peace and security.

The obligation to seek peaceful settlement of disputes does not preclude a state's inherent right for self-defence in response to an armed attack, the right for taking lawful countermeasures, or other lawful action.

Retorsion

Retorsions may be taken as a response to malicious cyber operations as long as they are not in violation with international law.

Retorsions will remain as measures for a state to respond to unfriendly acts or violations of international law, which by themselves do not constitute a

countermeasure. States have the right to apply these measures as long as they do not violate obligations under international law.

These measures could, for example include the expulsion of diplomats or applying restrictive measures to officials of a third country such as asset freezes or travel bans. One example of such a mechanism would be the European Union's cyber sanctions regime and cyber diplomacy toolbox, which offer an array of measures that could be taken as a response to malicious cyber operations.[6]

Countermeasures

If a cyber operation does not reach the threshold of armed conflict but nonetheless constitutes a violation of international law, states maintain the right to take countermeasures, in accordance with the law of state responsibility.

Countermeasures have strict legal criteria — an injured state may only take countermeasures against a state that is responsible for an internationally wrongful act in order to induce the given state to comply with its international obligations. This means that under certain circumstances, an injured state has the right to take measures that would normally violate international customary law or international treaties, but taken as a countermeasure such actions would be permitted as they would be in response to a violation of international law.

In order to take countermeasures in response to a malicious cyber operation violating international law, the operation in question must have been attributed to a state.

Right to self-defence

In accordance with Article 51 of the UN Charter, states have the right for self-defence in the case of an armed attack.

In order to assess if a cyber operation reaches the threshold of the use of force or an armed attack based on Article 2(4) or 51 of the UN Charter, we must consider the scale and effects of the operation. If the effects of a cyber operation are comparable to a kinetic attack, it could constitute an armed attack.

In such a situation, the injured state has the right to self-defence considering all applicable restrictions of the UN Charter and customary international law, such as proportionality and necessity.

[6] Draft Council of the European Union Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities ("Cyber Diplomacy Toolbox") (2017): https://data.consilium.europa.eu/doc/document/ST-9916-2017-INIT/en/pdf; Council of the European Union Decision concerning restrictive measures against cyber-attacks threatening the Union or its Member States (2019): https://data.consilium.europa.eu/doc/document/ST-7299-2019-INIT/en/pdf

In its response to an armed attack by cyber means, the injured state is not necessarily limited to taking measures by cyber means — all means remain reserved to states in order to respond to an armed attack in a manner that is proportionate and in accordance with other provisions of international law.

Estonia believes that cyber operations that cause injury or death to persons, damage or destruction could amount to an armed attack under the UN Charter.

IV. Conclusions

International law remains essential to relations between states for setting clear boundaries on what is and is not acceptable behaviour in cyberspace. Alongside other elements of the cyber stability framework, international law provides overarching guidance as to states' international rights and obligations applicable to cyberspace.

A clear need for deepening the understanding on how international law applies to cyberspace has been noted during discussions between states. We welcome the publication of expert and national views and work done by states as well as other stakeholders, including academia and relevant organisations.[7]

Estonia is looking forward to further constructive exchanges of views, including under the auspices of the UN, on how international law applies to state use of ICTs. The UN is an inclusive and necessary format to enable substantive discussions on responsible state behaviour in cyberspace. States should also engage with all stakeholders, including the private sector, civil society and academia, to discuss international law issues. One possible and helpful avenue for further awareness raising on how existing international law applies in cyberspace could be as part of a permanent Programme of Action (PoA) under the auspices of the UN First Committee.

[7] For example, the work done by the International Committee of the Red Cross on the application of international humanitarian law (IHL) to cyber operations during armed conflicts is commendable and can help with further study on how IHL principles apply in cyberspace.