Estonian positions — 2021-25 United Nations Open-Ended Working Group on "Developments in the Field of Information and Telecommunications in the Context of International Security"

Purpose

This paper sets out Estonia's objectives during the United Nations Open-ended Working Group (OEWG), established pursuant to resolution 75/240, and offers some concrete examples of initiatives for supporting the maintenance of stability in cyberspace and preventing conflict stemming from malicious cyber activities. Estonia believes that the OEWG should focus on the following issues as a matter of priority: 1) deepening understanding on how existing international law applies in cyberspace and acting as a platform for a more granular exchange of views; 2) considering practical opportunities to support the implementation of the 11 norms of responsible state behaviour in cyberspace, building on the additional layer of understanding offered by the 2021 Group of Governmental Experts (GGE) report; 3) highlighting regional efforts and supporting the development and operationalisation of confidence-building and transparency measures, 4) identifying the urgent cybersecurity needs of states and joining the dots for impactful cyber capacity building; 5) harnessing the expertise of the multi-stakeholder community.

Background

Deliberations in the United Nations First Committee have allowed to make substantial progress in clarifying obligations and expectations for states in their activities in cyberspace. Notably, the work of the UN Groups of Governmental Experts (GGE) since 2004 has allowed to outline and agree on a solid and effective framework for responsible state behaviour in cyberspace. This consists of existing international law, eleven voluntary non-binding norms, confidence-building measures and capacity building. In particular, the 2013 consensus report affirmed the application of international law in cyberspace[1]; the 2015 consensus report, while reaffirming this, additionally set out eleven voluntary non-binding norms of responsible state behaviour in cyberspace including several norms on critical infrastructure protection[2], while the 2021 consensus report furthermore reaffirmed the acqui and provided an important additional layer of understanding to these norms alongside important recommendations related to confidence-building measures and capacity building.[3] Since 2009, a representative from Estonia has been elected to be part of all consecutive UN Groups of Governmental Experts (GGE). The 2019-2021 Open-ended Working Group (OEWG) provided an important complementary forum, allowing all UN Member States to exchange

[1] A/68/98*, adopted by consensus with UN General Assembly Resolution A/RES/68/243
[2] A/70/174, adopted by consensus with UN General Assembly Resolution A/RES/70/237
[3] A/76/135, approved by consensus UN First Committee draft document A/C.1/76/L.13

views on threats stemming from the malicious use of cyberspace and concluding in a substantial consensus report which reaffirmed the existing framework and provided a number of key recommendations, such as a comprehensive list of capacity-building principles that states should consider in their efforts.[4] The consensus report was accompanied by a Chair's Summary which noted an array of initiatives that are not part of the UN consensus yet but which could merit further study. The GGE reports and OEWG report have been welcomed by consensus resolutions.

This paves the way for discussions in the 2021-2025 Open-ended Working Group (OEWG), established pursuant to resolution 75/240, and acts as a solid basis for further work.

Priorities for Estonia during the OEWG 2021-2025

1) Deepening understanding on how existing international law applies in cyberspace:

States should strive to deepen a common understanding of how existing international law applies in cyberspace, alongside its possible implications and legal consequences. Continuing such exchanges is clearly recommended by the 2021 OEWG[5] and GGE[6] reports, and the 2021-25 OEWG could act as one platform for a more granular exchange of views. Topics for study could include peaceful settlement of disputes, attribution and the law of state responsibility regarding internationally wrongful cyber operations, and the application of international human rights law in relation to state conduct in cyberspace. The 2021 GGE report for the first time also mentioned international humanitarian law and identified questions related to established legal principles including the principles of humanity, necessity, proportionality and distinction noted in the 2015 GGE report as one specific topic for further study. Underscoring that recalling these principles by no means legitimises or encourages conflict, the OEWG should further study on how these principles apply to the use of information and communication technologies (ICTs) by states. Estonia has published its views on how international law applies in cyberspace, most recently as part of the 2021 GGE official compendium (A/76/136)[7], and continues to encourage states to share their views and assessments on these topics, including through submissions to the UN Secretary-General and other avenues.

2) Supporting practical opportunities for norms implementation:

While highlighting that norms do not replace or alter States' obligations or rights under international law, Estonia considers that the 11 voluntary, non-binding

[4] A/75/816, agreed by UN General Assembly Decision 75/564 and approved by consensus UN First Committee draft document A/C.1/76/L.13
[5] Paragraphs 38-40, A/75/816
[6] Paragraph 72, A/76/135
[7] See Annex

norms of responsible state behaviour, set out in the 2015 GGE report and given an important additional layer of understanding in the 2021 GGE report, 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. Exchanges in the OEWG could allow to elaborate on and strengthen these norms, building on the additional layer of understanding provided by the latest GGE report, further clarifying the expectations that the norms reflect and considering practical opportunities to support states in norm implementation. One concrete example includes discussions that would contribute to the further development of the national survey of implementation of the UN General Assembly Resolution 70/237, which emerged as one practical outcome from the latest OEWG and GGE reports[8], or other such initiatives that allow to identify existing efforts and needs for norm implementation. While all eleven norms are important and form a package, given the urgency of preventing damage to critical infrastructure stemming from malicious cyber activities, specific additional attention could be given in particular to initiatives related to the norms pertaining to critical infrastructure protection (norm 13 (f) and norm 13 (h)). The role of different stakeholders in norm implementation should be further elaborated, with the aim of advancing common understandings on respective responsibilities and providing future guidance, as well as in view of taking into account gender considerations in cybersecurity.

3) Highlighting the regional dimension and advancing confidence-building measures:

Cybersecurity demands a national and regional approach in order to be successful on a global level. The latest OEWG and GGE reports both acknowledge the importance of the regional dimension, including the role played by regional and sub-regional organisations, in taking forward the assessments and recommendations reached in the UN (such as the GGE reports) and putting in place specific region-specific measures to build confidence and establish new avenues for cooperation and mutual learning.[9] Estonia continues to stand for the consideration of the regional dimension throughout the OEWG discussions and encourages meaningful consultation and timely information sharing with regional stakeholders (such as the EU, OSCE, OAS, ASEAN Regional Forum). This would offer the opportunity to provide practical tools and share lessons learnt and best practices on existing cybersecurity strategies and confidence-building measures (CBMs), further encourage and advance the development and implementation of these CBMs and allow to explore mechanisms for cross-regional exchanges of lessons and good practices on CBMs. Specific areas of focus could include continuing exchanges on cooperative and transparency measures related to

[8] Paragraph 65, A/75/816; Paragraph 86 (h), A/76/135. Initial co-sponsors of the „National Survey of Implementation of United Nations General Assembly Resolution 70/237" were: Argentina, Australia, Canada, Chile, Denmark, Estonia, France, Indonesia, Kenya, Mexico, the Netherlands, New Zealand, Pacific Island Forum member states, Poland, and South Africa. Many delegations subsequently expressed support for the proposal during 2019-2021 OEWG virtual meetings.
[9] Paragraphs 45-47, 52-53, A/75/816; Paragraphs 4, 17, 74-86, etc, A/76/135

critical infrastructure protection, the role of the broader multi-stakeholder community including the private sector, academia and civil society in facilitating such engagement, as well as the appointment of dedicated Points of Contact at the policy, diplomatic and technical levels, based on the assessments and recommendations of the latest OEWG and GGE reports[10], and initiatives from the OEWG Chair's Summary such as the viability of establishing a global directory of PoCs.[11]

4) Identifying state needs and joining the dots for impactful cyber capacity building:

The latest OEWG and GGE reports both attach great importance to capacity building and international cooperation. Estonia regards cyber capacity building as a priority area in order to improve the overall resilience of countries against malicious cyber activities and allow to implement the recommendations reached at the UN level. There is already an array of cyber capacity building activities, such as the Global Forum on Cyber Expertise, the World Bank's Cybersecurity Multi-Donor Trust Fund, EU CyberNet and other activities by the European Union, the work done by the OSCE and its field operations, as well as national initiatives. However, more could be done to identify functional and geographical gaps within existing efforts. The OEWG could act as a platform to provide an overview of and present lessons learnt from existing activities as well as identify and discuss the needs of states that could be addressed as a matter of priority. Furthermore, taking into consideration and further elaborating upon widely accepted principles, the 2019-2021 OEWG agreed on a list of principles by which capacity-building in relation to State use of ICTs in the context of international security should be guided, divided into three categories (Process and Purpose, Partnerships, People). The new OEWG could strive to further discuss these principles, such as the principle that capacity-building should respect human rights and fundamental freedoms and be gender sensitive and inclusive, and develop further content to support their implementation.[12] In parallel, this should be accompanied by communication and consultation with the wider multi-stakeholder community in order to broaden the support for these principles, raise awareness of them, and seek further input.

5) Harnessing the expertise of the multi-stakeholder community:

Given the role of the multi-stakeholder community in ensuring the maintenance of an open, free and secure cyberspace and their expertise and close relation to the topics under discussion in the OEWG, the meaningful, regular and substantial participation of the private sector, civil society and academia should to be one of the key objectives of the OEWG. While a level of engagement in the previous OEWG through informal consultations and events was achieved thanks to the

[10] Paragraph 47, A/75/816; Paragraphs 76-78, A/76/135
[11] Paragraph 30, 2019-2021 OEWG Chair's Summary
[12] Paragraph 56, A/75/816

efforts of the Chair and a number of Member States, the new OEWG should go further and create modalities that ensure that more non-governmental stakeholders can meaningfully participate in formal OEWG meetings than was the case for the previous OEWG (i.e. not solely tied to ECOSOC status), information would be shared with non-governmental stakeholders in a timely manner, non-governmental stakeholders would be granted sufficient time and flexible formats of participation to express their views and for delegations to discuss those views, multi-stakeholder input from all interested parties would be made readily available for all delegations in order to be granted due consideration throughout the OEWG process. Multi-stakeholder inclusion in the UN has a considerable history, and other inclusion processes could be consulted and drawn upon in order to analyse their feasibility in the context of cybersecurity discussions.[13]

Concrete examples of initiatives

Estonia is committed to sharing practical examples and exchanging best practices to support the implementation on the framework for responsible state behaviour, such as establishing cyber-resilient systems and cyber policies in keeping with human rights and fundamental freedoms, ensuring the protection of critical infrastructure from malicious cyber activities. There are a wealth of practical initiatives already available or being developed and the below is intended to provide only a very small sample of efforts.

International law:

- **Sharing views on how international law applies in cyberspace, including with the UN Secretary-General and the UN Cyber Policy Portal**: In recent years, an increasing number of states have published their positions on how international law applies in cyberspace. This is an important measure to deepen common understandings, increase predictability, transparency and prevent conflict in cyberspace. The OEWG report recommended that States, on a voluntary basis, continue to inform the Secretary-General of their national views. The latest GGE report was accompanied by an official compendium of voluntary national contributions on the topic by participating experts (A/76/136) and encouraged states to continue sharing their national views and assessments voluntarily through the United Nations Secretary-General and other avenues as appropriate. For example, Estonia has made its positions available on the UN Cyber Policy Portal, the website of the Ministry of Foreign Affairs, and in the GGE official compendium.
- **Tallinn Manual:** The Tallinn Manual 1.0 on the International Law Applicable to Cyber Warfare and the Tallinn Manual 2.0 on the International Law

[13] Some examples and options are included in „Multistakeholder participation at the UN: The need for greater inclusivity in the UN dialogues on cybersecurity", a study by Paris Call Working Group 3 on Advancing the UN negotiations with a strong multistakeholder approach (November 2021, Cybersecurity Tech Accord): https://pariscall.international/assets/files/10-11-WG3-Multistakeholder-participation-at-the-UN-The-need-for-greater-inclusivity-in-the-UN-dialogues-on-cybersecurity.pdf

Applicable to Cyber Operations are the flagship research initiative of the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) based in Tallinn, Estonia and is considered one of the most comprehensive academic analyses on how existing international law applies to operations in cyber space. The Tallinn Manual 3.0 process has started, which will revise and expand the 2017 edition, Tallinn Manual 2.0, in light of State practice and statements on the applicability of international law to cyber operations. Experts around the world are invited to contribute to the process.

- **Cyber Law Toolkit**: The Cyber Law Toolkit of the NATO CCDCOE is a dynamic interactive web-based resource for legal professionals who work with matters at the intersection of international law and cyber operations. At its core, it presently consists of 25 hypothetical scenarios. The project is supported by the following six partner institutions: the Czech National Cyber and Information Security Agency (NÚKIB), the International Committee of the Red Cross (ICRC), the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), the University of Exeter, United Kingdom, the U.S. Naval War College, United States, and Wuhan University, China. The individual scenarios and the Toolkit have been reviewed by a team of over 30 peer reviewers. The Toolkit was formally launched at the 11th annual Conference on Cyber Conflict (CyCon) in Tallinn, Estonia in 2019 and remains continuously updated, having a new additional feature of combining national statements by States on how international law applies in cyberspace.

Norms:

- **Programme of Action proposal:** The Programme of Action was one of the most concrete proposals to emerge from the 2019-2021 OEWG discussions. Currently co-sponsored by 54 States (including Estonia)[14] but actively seeking engagement and input from any interested party, a Programme of Action would be an inclusive and action-based platform aimed at advancing concrete cooperation against the malicious use of ICTs. It would focus on implementing the framework for responsible state behaviour in cyberspace, supporting capacity building and providing meaningful multi-stakeholder participation. To that end, informal consultations for its establishment will take place in different venues and fora, which could also provide an opportunity to hear the views of non-governmental organisations. The new OEWG could also provide the opportunity for inclusive and open discussions on this initiative.
- **Survey of National Implementation**: The voluntary "National Survey of Implementation of United Nations General Assembly Resolution 70/237"

[14] Argentina, Australia, Austria, Belgium, Bulgaria, Canada, Chile, Colombia, Croatia, Cyprus, Czech Republic, Denmark, Ecuador, Egypt, Estonia, France, Finland, Gabon, Georgia, Germany, Greece, Guatemala, Hungary, Iceland, Ireland, Italy, Japan, Latvia, Lebanon, Liechtenstein, Lithuania, Luxembourg, Malta, Morocco, Montenegro, Netherlands, Norway, Poland, Portugal, Republic of Korea, Republic of Moldova, Republic of North Macedonia, Romania, Salvador, Singapore, Slovakia, Slovenia, Spain, Sweden, Switzerland, Ukraine, United Arab Emirates, United Kingdom.

was included in both the OEWG and GGE reports. Its establishment in an interactive platform could provide a convenient and time-efficient measure for States to report on their implementation efforts and help map out potential gaps.

- **UNIDIR Cyber Policy Portal:** The interactive UNIDIR Cyber Policy Portal, first launched in 2019, is an important resource and reference tool that maps the global cyber policy landscape for policymakers and experts. It provides concise yet comprehensive cybersecurity policy profiles of all 193 UN Member States, as well as regional and international organisations and multilateral frameworks. Making further use of it for updates and analysis on norm implementation could be considered.
- **Paris Call:** The Paris Call for Trust and Security in Cyberspace was launched in 12 November 2018 with the aim of bringing all cyberspace actors together to face the new threats endangering citizens and infrastructure. The supporters of the Paris Call commit to working together to adopt responsible behaviour and implement within cyberspace the fundamental principles which apply in the physical world. To date, the Paris Call has attracted over 1,200 supporters, including over 75 national governments. In 2020, six multi-stakeholder working groups were launched under the Paris Call and presented their work as part of the Paris Peace Forum in November 2021.

Confidence-building measures:

- **Regional efforts in developing and operationalising CBMs:** Regional organisations are well equipped to develop and implement Confidence-Building Measures (CBMs), allowing for practical, long-term activities to build trust in smaller settings, all the while contributing to global peace and security. Since 2013, OSCE participating States have adopted 16 Cyber/ICT Confidence Building Measures (CBMs) which offer concrete tools to enhance interstate transparency, communication, and co-operation in cyberspace. The operationalisation of these CBMs have been supported by the "Adopt a CBM" programme of the Chair of the OSCE Informal Working Group which has permitted activities under a number of the CBMs to be spearheaded by specific participating States on a voluntary basis. Important developments in relation to CBMs are taking place in the ASEAN Regional Forum (ARF) and the Organization of American States (OAS).[15] While there are States who are not part of a regional organisation, positive developments to allow for more inter-regional exchange on CBMs (such as in the OSCE framework) should be welcomed and further explored.
- **Global repository of PoCs:** The idea of establishing a global repository of Points of Contacts (PoCs) was discussed during the 2019-2021 OEWG and

[15] A comprehensive overview on existing CBMs is provided by „Overview Of Existing Confidence Building Measures As Applied To Cyberspace" (The Global Forum on Cyber Expertise, 03/06/2020): https://cybilportal.org/wp-content/uploads/2020/05/GFCE-CBMs-final.pdf

included in the Chair's Summary.[16] This could be further explored, while noting that the security of such a directory as well as its operational modalities would be crucial to its effectiveness, as would avoiding duplicative or overly detailed arrangements. The value of regularly conducting exercises among a network of PoCs was also emphasised, as it can help to maintain readiness and responsiveness and ensure that PoC directories remain updated.

Capacity-building:

- **EU CyberNet and the Latin America and the Caribbean Cyber Competence Centre**: Launched in 2019, EU CyberNet bridges expertise across the European Union (EU) and establishes a network and a practical learning platform for strengthening cybersecurity globally. One of the core goals is strengthening the global delivery, coordination and coherence of the European Union's external cyber capacity building projects. The project is funded by the European Commission and implemented by the Estonian Information System Authority, in cooperation with the Advisory Board partners — the Federal Foreign Office of Germany and the Cybersecurity Competence Centre of Luxembourg. A concrete initiative of EU CyberNet is supporting the establishment of a regional cyber competence centre in Latin America. While other regions have at least some such initiative (e.g. the NATO Cooperative Cyber Defence of Excellence established in 2009, the ASEAN-Singapore Cybersecurity Centre of Excellence established in 2019, Cybersecurity Capacity Centre for Southern Africa established in 2020), there is currently no regional centre in Latin America and the Caribbean. The Latin America and the Caribbean Cyber Competence Centre (LAC4) is in the process of being established and will be operational in 2022, with the physical training facility in Santo Domingo, the Dominican Republic. The centre will be a regional knowledge hub and training centre that covers the full range of cybersecurity needs of the regional participants, reaching out to regional experts, providing technical, policy and strategic level courses and simulation. From this cooperation, other related initiatives have emerged, such as supporting, in cooperation with the EU's Cyber4Development project, the Dominican Republic authorities to conduct the first national cybersecurity exercise "Ciber Llamas".
- **The Global Forum on Cyber Expertise:** The Global Forum on Cyber Expertise (GFCE) offers a pragmatic, action-orientated and flexible platform to strengthen international collaboration on cyber capacity building and expertise. Today, it is a multi-stakeholder community of more than 140 members and partners from all regions of the world. One of its core documents is the Delhi Communique on a GFCE Global Agenda for Cyber Capacity Building which prioritises 11 topics under 5 broad themes on cyber

[16] Paragraph 30, 2019-2021 OEWG Chair's Summary

capacity building and also enshrining a principle-based approach to implementing the Agenda. Its Cybil knowledge portal aims to be a one-stop global knowledge hub that brings together key information and lessons learnt on international cyber capacity building.

- **World Bank Cybersecurity Multi-Donor Trust Fund:** The World Bank's Cybersecurity Multi-Donor Trust Fund is developed as an associated trust fund under the broader Digital Development Partnership Umbrella (DDP). It aims to better define, understand, articulate, structure, and roll out the cybersecurity development agenda in a systematic manner. The emerging work programme will offer comprehensive cybersecurity capacity development, including development of global knowledge, country assessments, technical assistance, capacity building and training, underpinned with necessary investments in infrastructure and technology. The founding donors are Estonia, Germany, Japan, and The Netherlands.
- **The Tallinn Winter School of Cyber Diplomacy:** Organised by the Ministry of Foreign Affairs of Estonia in February 2021, the virtual training programme geared at newcomers to the field featured lectures and panel discussions by current and former cyber diplomats as well as experts from leading think tanks, academia and institutions and covered cover best practices of cyber norms implementation, the applicability of international law in cyberspace, and confidence and capacity building measures. It forms part of wider efforts on cyber diplomacy training, including on international law as recommended in the OEWG and GGE reports.

Conclusion

Estonia looks forward to continuing to engage constructively in regular institutional dialogue under the auspices of the UN and considers that the OEWG can provide a valuable platform to deepen understanding of different national and expert views on international cyber security. Estonia stresses the importance of the OEWG operating on the basis of consensus modalities, with elements such as the Programme of Work to be decided on this basis and to be subject to mid-term review. Furthermore, Estonia supports the consideration of additional forums and mechanisms to take agreed consensus forward and provide practical support for implementation.

ANNEX

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[17] and reaffirmed by the OEWG consensus report.[18] 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

[17] 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
[18] A/75/816, adopted by UN General Assembly Decision A/DEC/75/564

regarding internationally wrongful acts attributable to them under international law; 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; 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."[19] 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).

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

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 threat or use of force against the territorial integrity or political independence of any State [...]."[20]

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

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

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.

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.[21]

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

[21] 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

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.

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.[22]

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

[22] 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 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.

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.[23]

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.

[23] 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.