https://doi.org/10.25143/socr.24.2022.3.030-040

Applicability of International Law in Cyberspace: Positions by Estonia and Latvia

Mg. sc. pol. ***Laura Done***
ORCID: 0000-0003-4246-3137
Rīga Stradiņš University, Latvia
laur.done@gmail.com

Abstract

The study focuses on applicability of international law in cyberspace, particularly on the global processes at the United Nations Committee on Disarmament and International Security and analyses whether and how Estonia and Latvia understand and explain the application of international law to the states' conduct in cyberspace.

The aim of the study is to provide qualitative and comparative analysis on what national positions Estonia and Latvia have on applicability of international law in cyberspace and how these opinions are reflected in their national cybersecurity strategies and national statements. The article assesses the efforts by Estonia and Latvia to promote understanding on how international law applies in cyberspace. These efforts are analysed from foreign policy perspective. The article also argues why it is crucial to promote such an understanding; however, it does not discuss or interpret legal concepts.

The article concludes with a comparison of the cases of Estonia and Latvia. The result of the research indicates that Estonia has been more active than Latvia in terms of defining and promoting its official position on applicability of international law in cyberspace. Latvia has not yet provided detailed positions on applicability of international law in cyberspace.

Keywords: cybersecurity, cyberspace, international law, international security, international society.

Introduction

With the constant development of information and communication technologies (ICTs), the issue of their application and related security risks is also becoming relevant. Although ICTs and a range of other emerging and revolutionary technologies bring

significant benefits to individuals and societies, for instance, in terms of communication, access to services and business, they also play an essential, and sometimes negative, role in international relations.

The use of ICTs by states for military purposes and the increase of state-sponsored cyber-attacks for espionage, theft of intellectual property and other malicious and disruptive activities raise serious concerns not only about the protection and resilience of ICTs systems, but also about the irresponsible state behaviour in cyberspace. Some states are using cyber-attacks as part of a wider hybrid warfare to influence an adversary. Such malicious and disruptive cyber-activities orchestrated by one state against another can threaten international peace and security. At the global level, states are increasingly discussing international cybersecurity issues, including international law, norms and principles states should adhere to when using ICTs.

In the United Nations (UN) Committee on Disarmament and International Security (also known as the First Committee), states have been discussing ICTs issues in the context of international security since 2004 when the UN Group of Governmental Experts (UN GGE) began its work. Such discussions, but in the framework of a new expert group, namely UN Open-Ended Working Group (UN OEWG), are expected to continue until 2025. Since 2004, states have been actively working together to understand whether and how the international law applies to cyberspace, including when states are using ICTs (the behaviour of states in cyberspace). In less than twenty years, progress has been made in recognising the application of existing international law in cyberspace, including the UN Charter and human rights principles, as well as various other non-binding rules and principles. The attempts to reach a common understanding of applicability of international law in cyberspace have been only partially successful.

For example, different views over the aspects of countermeasures, self-defence and application of international humanitarian law still exist. Moreover, there are attempts by some states to review the decisions once made by the UN General Assembly on the applicability of international law in cyberspace. Authoritarian states do not fully share the view that existing international law is applicable in cyberspace and persistently suggest that there is a need for a new, binding international treaty that would regulate the states' conduct in cyberspace. Democratic states do not share such a view and keep promoting and strengthening the concept of applicability of already existing international law in cyberspace. Democratic states have concerns that through such a new, binding international treaty authoritarian states will restrict free flow of information and the governance model of cyberspace will become state centric, not human centric (Rosenbach & Chong, 2019). Democratic and like-minded states need to promote the concept that international law applies in cyberspace and take global discussions further in order to answer the question how it is applied.

The aim of the article is to examine how one of the most important outcomes of the work of UN GGE, notably stating that international law is applicable in cyberspace and is crucial to maintaining peace and stability (UN GGE, 2013), is reflected in current

national cybersecurity strategies and national statements of Estonia and Latvia at relevant UN GGE and UN OEWG meetings. The article provides qualitative, comparative, and, to a very limited degree, also legal analysis on Estonia's and Latvia's contributions on understanding on whether and how international law applies to the use of ICTs by the state. The qualitative analysis is performed by interpreting and analysing national cybersecurity strategies and national statements. The core issues of the article are analysed through foreign policy perspective. The article does not discuss or interpret legal concepts. The result of the research indicates that Estonia has been more active than Latvia in terms of defining and promoting its official position on applicability of international law in cyberspace. Latvia has not yet provided detailed positions on applicability of international law in cyberspace which may indicate lack of expertise and/or lack of human resources. If Latvia provided such an analysis and position, it would contribute to strengthening the understanding of the international community on the applicability of international law in cyberspace.

The article explains the global processes at the UN Committee on Disarmament and International Security in relation to responsible state behaviour in cyberspace and security of and in the use of information and communications technologies. The article examines Estonia's and Latvia's understandings of applicability of international law in cyberspace. It concludes with a comparison of the cases of Estonia and Latvia providing final conclusions.

1 Main Outcomes of UN GGE reports (2013–2021)

Early concerns that the misuse of ICTs could endanger international stability and security, rose in 1998, when Russia introduced a UN resolution on "Developments in the field of information and telecommunications in the context of international security" (UN doc. A/RES/53/70, 1999). Discussions on norms and laws which should govern the use of cyberspace became more prominent when the UN GGE was established in 2004.

The mandate of UN GGE has evolved over the years. For instance, in 2004 the group's mandate was:

> "*Requests the Secretary-General to consider existing and potential threats in the sphere of information security and possible cooperative measures to address them, and to conduct a study on the concepts referred to in paragraph 2 of the present resolution, with the assistance of a group of governmental experts [..].*" (UN doc. A/RES/58/32, 2003)

The latest UN GGE group in 2018 was mandated to:

> "*[..] to continue to study, with a view to promoting common understandings and effective implementation, possible cooperative measures to address existing and potential threats in the sphere of information security, including norms, rules and principles of responsible behaviour of States, confidence-building measures and capacity-building, as well as how international law applies to the use of information and communications technologies by States [..].*" (UN doc. A/RES/73/266, 2018)

Adjustments and evolutions of the mandate are in line with the findings and recommendations of the UN GGE reports in 2013, 2015 and 2021.

Until now there have been six UN GGE. Usually, the group works for two years, it has at least 2 working sessions per year. The groups have consisted of 15–25 experts. The main outcome of working sessions is consensus reports which include findings and, most importantly, recommendations for states to guide their conduct in cyberspace. The recommendations are non-binding, but, mostly, have been well recognised by the UN member states and some of them even adopted by consensus. In total, the groups have produced four reports. The most prominent and fundamental findings and recommendations are included in 2013 and 2015 reports. (UN, 2021)

In 2013, the UN GGE report concluded that international law applies in cyberspace; state sovereignty applies to State conduct of ICTs; human rights and fundamental freedoms must be respected in cyberspace:

> "*19. International law, and in particular the Charter of the United Nations, is applicable and is essential to maintaining peace and stability and promoting an open, secure, peaceful and accessible ICT environment.*
> *20. State sovereignty and international norms and principles that flow from sovereignty apply to State conduct of ICT-related activities, and to their jurisdiction over ICT infrastructure within their territory.*
> *21. State efforts to address the security of ICTs must go hand-in-hand with respect for human rights and fundamental freedoms set forth in the Universal Declaration of Human Rights and other international instruments."* (UN doc. A/68/98*, 2013)

After the report in 2013, the UN GGE continued its work, building upon work that had been done previously and concluded its work with a new consensus report in 2015. The report of UN GGE in 2015, among other things, offers eleven key recommendations for voluntary, non-binding norms, rules or principles of responsible behaviour in cyberspace (UN doc. A/70/174).

One of the key recommendations is:

> "*States should not knowingly allow their territory to be used for internationally wrongful acts using ICTs.*" (UN doc. A/70/174, 2015)

Recommendations suggest that states should not conduct or knowingly support malicious ICT activities and such activities should be mitigated if emanating from their territory and are directed against another state (UN doc. A/70/174, 2015). The report also provides deeper insights on how international law applies to states' conduct in cyberspace. Mainly, it reflects discussions on sovereignty, confirming that:

> "*States have jurisdiction over the ICT infrastructure located within their territory.*" (UN doc. A/70/174, 2015)

The group concluded that there is a need for continued discussions to improve the understanding of how international law applies in cyberspace, including on countermeasures which states can implement according to the UN Charter. The report also highlights the challenges of attribution.

In 2017, UN GGE failed to agree on a consensus report because of different views over the aspects of countermeasures, self-defence, due diligence, application of international humanitarian law and sovereignty (Tikk & Kerttunen, 2017). The group resumed the work in 2019 and provided a consensus report in 2021. The report addresses the issue with the application of international humanitarian law, noting that IHL is applicable in cyberspace but only during an armed conflict (UN doc. A/76/135, 2021). Normative clarifications regarding due diligence and sovereignty still need to be addressed.

There is a separate document accompanying UN GEE report 2021:

> "*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 73/266*".

This compendium consists of national views on how international law applies to states' conduct in cyberspace submitted by UN GEE participating states. Apart from the Compendium 2021, since the establishment of UN GEE, UN member states are regularly invited by resolutions to inform the UN Secretary General of their opinions and positions on concepts covered by the UN GGE recommendations. It also refers to states' views and assessments of how international law applies in cyberspace.

UN Resolution A/RES/73/27 in 2018 introduced a new group called Open-ended Working Group (UN OEWG) with almost the same mandate as UN GGE. UN OEWG is a Russian led initiative, open to all UN member states, while UN GGE members are selected based on candidatures. The group concluded its first report in 2021 and is expected to continue its work till 2025. The report does not contribute meaningful, new recommendations on how international law applies in cyberspace. Nevertheless, it was crucial that the UN OEWG reaffirmed the work done by UN GGE in 2013 and 2015 (UN doc. A/AC.290/2021/CRP.2, 2021). The report is accompanied by "Compendium of statements in explanation of position on the final report" which reflects detailed positions of states on different issues, including controversial ones.

Although a lot has been achieved at the global level in terms of building norms and laws which should govern the use of ICTs by states in cyberspace, states must continue to discuss and to develop common understanding on how international law applies in cyberspace.

2 Applicability of International Law in Cyberspace: Cases of Estonia and Latvia

This section analyses national cybersecurity strategies. These are important policy documents which reflect what positions states have on different issues and also determine strategic guidelines. Additionally, national contributions to both compendiums (in the frameworks of UN GGE and UN OEWG 2021 reports) will be analysed, in order

to identify contributions of Estonia and Latvia. For the UN OEWG 2021 Compendium all UN member states were able to submit their positions, explaining their views on different issues expressed in UN OEWG report 2021. For the UN GGE 2021 Compendium only those states participating in the group were invited to submit their national views. Estonia is the only Baltics state which participated in the UN GGE 2019–2021. Latvia's contribution is not expected in the UN GGE Compendium. National statements expressed at relevant UN GGE and UN OEWG meetings will also be discussed.

Estonia

Estonia's current cybersecurity strategy (2019–2022) is a comprehensive document which defines strategic objectives of national cybersecurity policy. The document displays main areas of activities, including raising cyber awareness of society, promoting public and private partnerships, developing digital society, supporting research and development (Strategy, 2019–2022). Among these areas, there is a section dedicated to Estonia's role in the processes of shaping international law for cyberspace. Estonia sees herself as a credible and strong partner in this field at the global level. According to the current cybersecurity strategy (Strategy), cyber is part of Estonia's foreign policy, especially international cooperation on cyber norms and international law. The state also acknowledges that discussions on the application of international law in cyberspace are essential and complicated ones at the global level (Strategy, 2019–2022). In its Strategy, Estonia demonstrates readiness to be involved in cooperation regarding UN GGE and UN OEWG unresolved issues, for instance, attribution of attacks and countermeasures (Strategy, 2019–2022). In Strategy, Estonia has expressed intentions to create an international cyber law centre in order to develop even more competency, particularly on the civilian side of international law (Strategy, 2019–2022). The Strategy concludes that there is a need to achieve a consensus on how international law applies in cyberspace. The Strategy also defines that Estonia must continue its active participation in the UN cyber processes. In the Strategy, Estonia emphasizes its role in the fact that the number of states that recognise the applicability of international law in cyberspace has increased (Strategy, 2019–2022).

Estonia has been a regular UN GGE participant and with its expertise has contributed to all four consensus reports. Estonia sees UN GGE as a global, high-level forum for cyber norms discussions and participation in the UNGGE is one of the foreign policy priorities (Kaljurand, 2016). Estonia decided to apply for UN GGE membership only in 2008 (Kaljurand, 2016), and not in 2003, potentially because of experienced cyber-attacks to its government websites and online services in 2007.

Estonia has extensively contributed to the UN GGE Report 2021 annex: "*Compendium of voluntary national contributions on the subject of how international law applies to the use of information and communications technologies [..]*". In its position, Estonia reaffirms its view that existing international law applies in cyberspace and that there is no need for new, binding treaties. In its position Estonia provides explicit views on pressing issues like sovereignty, due diligence, attribution, countermeasures, international humanitarian law etc. (UN GGE Compendium, 2021)

For example, regarding due diligence it is still unclear whether it is a legal obligation or not (Kaljurand, 2016), but in its position Estonia justifies that:

> "*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.*" (UN GGE Compendium, 2021)

And:

> "*Without this obligation international law would leave injured states defenceless in the face of malicious cyber activity that emanates from other states' territories.*" (UN GGE Compendium, 2021)

Such a detailed national position helps to improve the understanding of the applicability of international law in cyberspace for those states that lack expertise in legal aspects of cybersecurity. To a number of states (so-called Non-Aligned Movement states) it is not yet clear which of the positions and approaches to choose, meaning to support or object the notion that international law is applicable in cyberspace. In order to persuade such states to support one position or another, diplomatic activities are implemented by authoritarian states and democratic and like-minded states. Given the conflicting ideological visions of how cyberspace should be governed, the diplomacy chosen and pursued by countries is important in resolving conflicting issues.

Estonia has also contributed to the UN OEWG Report 2021 annex: "*Compendium of statements in explanation of position on the final report".* The statement contains some of already expressed positions and is more oriented on sharing the views on the UN OEWG final report. In its statement it reaffirms the applicability of international law in cyberspace:

> "*This includes the Charter of the United Nations in its entirety, customary international law, human rights law and international humanitarian law, all of which apply in cyberspace.*" (UN OEWG Compendium, 2021)

Estonia urges for further in-depth discussions on the applicability of international law in cyberspace. Estonia also encourages states to develop their national positions on how exactly existing international law applies in cyberspace (UN OEWG Compendium, 2021).

Estonia has been developing its position on the applicability of international law in cyberspace gradually at least since 2014 (Estonia's Contributions to the GGE, 2014). Estonia considers that it is crucial to continue to develop a common understanding of how international law applies in cyberspace (UN GGE Compendium, UN OEWG Compendium, 2021).

Latvia

Latvia's current cybersecurity strategy (2019–2022) defines vision, objectives, priorities, and fundamental principles of national cybersecurity policy. It describes functions and responsibilities of state institutions. In the case of Latvia, cybersecurity is part of

comprehensive national defence (Strategy of Latvia, 2019–2022). The document presents main areas of activities: promoting cybersecurity; strengthening resilience of ICTs; raising public awareness; supporting education and research; strengthening international cooperation; ensuring rule of law in cyberspace etc. (Strategy of Latvia, 2019–2022). The Strategy states that it is necessary to deepen cooperation with partners to achieve common understanding of cyberspace in general. The section of international cooperation, which is the only one which includes reference to international law, mainly focuses on the EU and NATO aspects.

Latvia acknowledges that there are challenges towards building a common understanding of cyberspace. The Strategy determines that:

> "*Together with like-minded countries, Latvia should try to promote shared and common global understanding of cyberspace and how international treaties apply to it.*" (Strategy of Latvia, 2019–2022)

In the Strategy's Latvian version the term "international norms" is used instead of "international treaties", which can be confusing. The Strategy supports the notion that existing international rules are applicable to both physical and virtual domains. The Strategy neither clearly expresses the position of applicability of international law in cyberspace, nor it expresses the views on the UN GGE processes. The English version uses vague terminology.

Latvia has not been a member of the UN GGE processes, which means that the state has not applied for membership or its candidature has been rejected by the UN Secretariat. The UN GGE is composed on the basis of equitable geographical distribution (The Digital Watch, 2021) which would mean competition with Estonia. Latvia was a participant of the UN OEWG 2019–2021, the group which is open to all UN member states.

Latvia has provided a contribution (statement) on the Zero and First draft of the UN OEWG report. Regarding international law, it states:

> *"[..] it is necessary to particularly emphasize the applicability of the UN Charter in its entirety since Charter is binding for all UN Member States and is essential to maintain peace, stability and promotion of open, secure and peaceful ICT environment."* (Statement by Latvia, UN OEWG, 2021)

In its statement, Latvia clearly affirms applicability of international law in cyberspace. In addition, it also urges further discussions on applicability of international law in cyberspace and reaffirms UN GGE report 2015 (Statement by Latvia, UN OEWG, 2021).

Conclusions

Establishment of laws, norms and principles governing the use of ICTs in cyberspace is still ongoing. The processes at the UN are highly politicised. There are two diverging visions on how cyberspace should be governed and by what laws states should be guided in use of ICTs in cyberspace. The UN General Assembly has affirmed that international

law applies in cyberspace. Remaining question is: how does it apply? Meanwhile, there are attempts by some states to review the decisions made by the UN GA and proposals to create new, binding treaties which would regulate cyberspace. Democratic states consider that through such proposals authoritarian states intend to restrict free flow of information, and the governance model of cyberspace would become state centric, not human centric.

Research shows that Estonia and Latvia both affirm and support the notion that international law is applicable in cyberspace, but Estonia has been more active than Latvia in terms of defining and promoting its official position on applicability of international law in cyberspace. Estonia has developed a detailed national position, addressing the most pressing and controversial concepts discussed at the UN GGE. Such a contribution helps to improve understanding of the applicability of international law in cyberspace for those states that lack expertise in legal aspects of cybersecurity, thus increasing support for the concept that international law is applicable in cyberspace. Overall, such a contribution helps to improve general understanding of the normative framework (norms, laws and principles) applicable in cyberspace. The ongoing processes at the UN level also have an implication for other international organisations, and a clear understanding of the violation of the normative framework is essential.

Estonia has been a regular UN GGE participant and with its expertise has contributed to all four consensus reports. Latvia has not been a member of the UN GGE processes but participated in the UN OEWG 2019–2021. In the case of Latvia, there is significantly fewer public materials and data to analyse. Latvia has not yet provided detailed positions on applicability of international law in cyberspace, even though it is encouraged by the UN Secretary General to do so. This may indicate a lack of expertise and/or a lack of human resources responsible for developing detailed positions on international cybersecurity policies. If Latvia provided such an analysis and position, it would contribute to strengthening the understanding of the international community on the applicability of international law in cyberspace. Although Latvia and Estonia are similar in terms of geography, military, economics, and territorial size, the role of cybersecurity in their foreign policies is fundamentally different. In the case of Estonia, cyber is part of its foreign policy, especially international cooperation on cyber norms and international law. The membership of the UN GGE has been a goal. Estonia promotes itself as the leading nation in the field and is keen to strengthen its expertise further. Estonia's ambitious cyber foreign policy and strong expertise have been developed since it suffered from state-sponsored cyber-attacks against its government websites and online services in 2007.

In-depth discussions are needed at the UN level to continue to build a common understanding of how international law applies in cyberspace.

Bibliography

1. Cybersecurity Strategy of Estonia 2019–2022. Available: https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/kyberturvalisuse_strateegia_2022_eng.pdf [rev. 05.05.2022].
2. Cybersecurity Strategy of Latvia 2019–2022. (17.09.2019). Available: https://www.mod.gov.lv/sites/mod/files/document/Cybersecurity%20Strategy%20of%20Latvia%202019_2022.pdf [rev. 05.05.22].
3. Estonia's Contributions to the GGE. (2014). Available: https://carnegieendowment.org/files/Estonia_UNGGE-input-paper_Sep2014.pdf [rev. 10.05.2022].
4. Kaljurand, M. (2016). United Nations Group of Governmental Experts: The Estonian Perspective. In *International Cyber Norms: Legal, Policy & Industry Perspectives*, p. 112–114. Available: https://ccdcoe.org/uploads/2018/10/InternationalCyberNorms_Ch6.pdf [rev. 10.05.2022].
5. Rosenbach, E., Chong, S. C. (2019). Governing Cyberspace: State Control vs. The Multistakeholder Model. Belfer *Center for Science and International Affairs, Harvard Kennedy School*. Available: https://www.belfercenter.org/publication/governing-cyberspace-state-control-vs-multistakeholder-model [rev. 16.05.2022].
6. Tikk, E., & Kerttunen, M. (eds.) (2017). *The Alleged Demise of the UN GGE: An Autopsy and Eulogy*. Cyber Policy Institute, p. 16–17. Available: https://cpi.ee/wp-content/uploads/2017/12/2017-Tikk-Kerttunen-Demise-of-the-UN-GGE-2017-12-17-ET.pdf [rev. 21.05.2022].
7. UN Conference room paper A/AC.290/2021/CRP.2 "Final Substantive Report". (10.03.2021). Available: https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf [rev. 19.05.2022].
8. UN, Developments in the field of information and telecommunications in the context of international security. Available: https://www.un.org/disarmament/ict-security/ [rev. 17.05.2022].
9. UN Document (A/76/136), 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 73/266 (A/76/136). (13.07.2021). Available: https://ccdcoe.org/uploads/2018/10/UN_-Official-compendium-of-national-contributions-on-how-international-law-applies-to-use-of-ICT-by-States_A-76-136-EN.pdf [rev. 21.05.2022].
10. UN General Assembly, Resolution A/RES/53/70, Developments in the field of information and telecommunications in the context of international security. (1999). Available: https://undocs.org/Home/Mobile?FinalSymbol=A%2FRES%2F53%2F70&Language=E&DeviceType=Desktop&LangRequested=False [rev. 05.05.2022].
11. UN General Assembly, Resolution A/RES/58/32, Developments in the field of information and telecommunications in the context of international security. (08.12.2003). Available: https://undocs.org/Home/Mobile?FinalSymbol=A%2FRES%2F58%2F32&Language=E&DeviceType=Desktop&LangRequested=False [rev. 08.05.2022].
12. UN General Assembly, Resolution A/68/98*, Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. (24.07.2013). Available: https://undocs.org/Home/Mobile?FinalSymbol=A%2F68%2F98&Language=E&DeviceType=Desktop&LangRequested=False [rev. 08.05.2022].

13. UN General Assembly, Resolution A/70/174, Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. (22.07.2015). Available: https://undocs.org/Home/Mobile?FinalSymbol=A%2F70%2F174&Language=E&DeviceType=Desktop&LangRequested=False [rev. 10.05.2022].
14. UN General Assembly, Resolution A/RES/73/266, Advancing responsible State behaviour in cyberspace in the context of international security. (2018). Available: https://undocs.org/Home/Mobile?FinalSymbol=A%2FRES%2F73%2F266&Language=E&DeviceType=Desktop&LangRequested=False [rev. 05.05.2022].
15. UN General Assembly, Resolution A/76/135, Report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security. (14.07.2021). Available: https://undocs.org/Home/Mobile?FinalSymbol=A%2F76%2F135&Language=E&DeviceType=Desktop&LangRequested=False [rev. 21.05.2022].
16. UN OEWG and GGE. Geneva internet platform. The Digital Watch. Available: https://dig.watch/processes/un-gge#Framework-of-responsible-behaviour [rev. 17.05.2022].