CHAPTER III

Aligning Estonian and Japanese Efforts in Building Norms in Cyberspace

Anna-Maria Osula

Introduction

The digital transformation of societies has expanded the attack surface, rendering malicious cyber activities a part of our everyday lives. According to some studies, cybercrime had cost the world €5.5 trillion by the end of 2020, up from €2.7 trillion in 2015, due in part to the exploitation of the Covid-19 pandemic by cybercriminals.[1] Alarmingly, the capabilities of cyber-threat actors are continuously advancing, with the attacks possibly inflicting serious damage or showcasing political motives, and thereby potentially threatening democratic processes such as elections.[2] Recent years have also witnessed increasing geopolitical concerns in areas such as connectivity, privacy and the free flow of information. Consequently, states are battling for a better position in both governing technologies and being at the forefront of technological innovation.

As a member of the European Union, Estonia broadly follows the rhetoric and direction of EU strategic objectives. With its new Cybersecurity Strategy, released in 2020, the EU confirms its ambition to be in the lead for the digital economy, to invest more in technology and to remain the frontrunner in maintaining a high level of protection for the whole of society.[3] Rules, regulations and norms have an important role to play in achieving this. Hence, the EU and Estonia continuously underline the applicability of international law and the importance of adhering to norms of state behaviour in cyberspace.

The EU and Estonia continuously underline the applicability of international law and the importance of adhering to norms of state behaviour in cyberspace

Japan is a key strategic partner for the EU in several important areas, cybersecurity being one of the domains identified for closer cooperation.[4] Japan has recently increased its focus on reinforcing cybersecurity both for public and private actors, keeping in mind the

[1] Igor Nai Fovino et al, *Cybersecurity, Our Digital Anchor* (Luxembourg: Publications Office of the European Union, 2020), 7, https://publications.jrc.ec.europa.eu/repository/bitstream/JRC121051/cybersecurity_online.pdf.

[2] ENISA, *ENISA Threat Landscape - The Year in Review* (Attika: European Union Agency for Cyber Security, 2020), 8, https://www.enisa.europa.eu/publications/year-in-review/at_download/fullReport.

[3] European Commission High Representative of the Union for Foreign Affairs and Security Policy, *The EU's Cybersecurity Strategy for the Digital Decade* (JOIN (2020)18 Final) (Brussels: European Commission, 2020), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020JC0018&from=EN.

[4] Council of the European Union, "Enhanced EU Security Cooperation in and with Asia: Council Conclusions," 9265/1/18 REV 1, 28 May 2018, https://www.consilium.europa.eu/media/35456/st09265-re01-en18.pdf; European Commission, "Annex 3 of the Commission Implementing Decision on the 2019 Annual Action Programme for cooperation with third countries to be financed from the general budget of the European Union: Action Document for 'Security Cooperation in and with Asia'," 2019, https://ec.europa.eu/fpi/sites/fpi/files/annexe_3_security_cooperation_in_and_with_asia_part1_v2.pdf.

Tokyo 2020 Olympic and Paralympic Games that should take place in the summer of 2021. Equally, recent Japanese cybersecurity strategies have underlined the role of cyber diplomacy, international cooperation and their close relationship with Japan's national security, and Japan is an avid supporter of the free flow of data.[5]

In light of Japan being a strategic partner for the EU in the cybersecurity domain, this chapter looks specifically at the cooperation between Estonia and Japan. While cybersecurity-related cooperation between the two countries began cautiously, the chapter examines recent developments in aligning the two countries' positions regarding building and promoting norms of state behaviour in cyberspace. In order to understand Estonia's unique position and to establish small states as credible partners in cyber diplomacy negotiations, the chapter will first set the scene by outlining the potential of small states to play a substantial role in taking the discussions on norms of state behaviour forward in international and regional fora. The chapter will then identify points of agreement and key similarities between Estonian and Japanese perspectives and offer suggestions for further cooperation.

1. Small States and Building Cyber Norms

Four pillars – international law, norms of state behaviour, confidence building and capacity building – form the backbone of current UN-level discussions on building and maintaining trust and security in the digital environment. International law and voluntary, non-binding norms of responsible state behaviour play a crucial role in clarifying state responsibilities in cyberspace. While international law is the foundation of stability and predictability in relations between states, norms play an important role in reflecting the expectations of the international community, reducing risks of misperceptions, and thus contributing to the prevention of conflict.[6] According to commentators, cyber norms and international law remain the best and most reliable way to build international security in cyberspace.[7]

International law and voluntary, non-binding norms of responsible state behaviour play a crucial role in clarifying state responsibilities in cyberspace

In particular, adherence to international law plays an important role in protecting small nations that cannot boast great military power or significant resources. In the words of Lennart Meri, Estonia's first post-Cold War president, "international law is the nuclear weapon of a small state".[8] Commonly agreed international legal norms provide clarity that allows states to foresee with certainty what actions would be considered as violating international law. International law also offers options for legal remedies to be used in the event of an offensive cyber operation being launched against a state. It is the assumption that such legal predictability, combined with other legal factors such as investigative measures, sanctions and a functioning judicial system, also acts as a deterrent against possible attacks.

Adherence to international law plays an important role in protecting small nations that cannot boast great military power or significant resources

[5] See: Government of Japan, *Cybersecurity Strategy 2018* (Tokyo: NISC, 2018), https://www.nisc.go.jp/eng/pdf/cs-senryaku2018-en.pdf. The Japanese Prime Minister Shinzo Abe proposed the concept of Data Free Flow with Trust at the Davos Meeting in 2019 and reiterated it at the G20 and G7 summits. See: Ministry of Foreign Affairs of Japan, "Speech by Prime Minister Abe at the World Economic Forum Annual Meeting," 23 January 2019, https://www.mofa.go.jp/ecm/ec/page4e_000973.html.

[6] See generally the UN GGE reports of 2013 and 2015, and: United Nations Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security, *Final Substantive Report* (A/AC.290/2021/CRP.2) (New York, NY: United Nations, 2021), https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf.

[7] James Lewis, "Overview of the Cyber Stability Framework: Norms of Responsible State Behaviour, International Law, Confidence and Capacity Building Measures," Tallinn Winter School of Cyber Diplomacy, 9–10 February 2021, https://vm.ee/et/node/53915.

[8] Lauri Mälksoo and Adam Lupel, "A Necessary Voice: Small States, International Law, and the UN Security Council," blog, ETH Zürich Center for Security Studies, 29 April 2019, https://css.ethz.ch/en/services/digital-library/articles/article.html.

However, this does not mean that small states necessarily exhibit a united position in defending the international legal order. In debates on state behaviour in cyberspace, small states are split by the same geopolitical fault lines as their bigger counterparts, and often disagree about the meaning and scope of application of international law. In the context of state behaviour in cyberspace, this can clearly be seen in the recent standoff at the United Nations, with Russia and the US proposing in 2018 two separate initiatives (respectively, the next iteration of the United Nations Group of Governmental Experts (UN GGE) and of the Open-Ended Working Group (OEWG)) to facilitate these discussions. While the UN General Assembly approved both proposals, the voting reflected the two opposing camps, largely falling along the lines of military and political alliances.[9] These two different groups also correspond to some of the debates over international law, such as the applicability of international humanitarian law to cyberspace. Despite the different views small states may have, the promotion of and commitment to the international rule of law is generally a common feature of their foreign policies and rhetoric.[10]

> *In debates on state behaviour in cyberspace, small states are split by the same geopolitical fault lines as their bigger counterparts*

> *Expertise and skilful diplomacy, developed in niche areas over time, can be used to achieve small states' strategic objectives*

Despite realpolitik arguments that powerful countries have more leverage in global politics, small states can prove effective in a number of ways. For example, their small size allows them to manoeuvre more quickly in policy debates, or adapt to technological change and innovation, without the constraints of large and static bureaucracies. In addition, when (human) resources are scarce, it makes sense to specialise on a strategic policy domain, build reputation and cultivate recognised expertise. This expertise and skilful diplomacy, developed in niche areas over time, can be used to achieve small states' strategic objectives as well as to provide "an important, credible voice with moral authority to remind all member states of their obligations under international law, reaffirm normative commitments to compliance, and advocate for a recommitment to a multilateral, rule-based order that is of collective benefit to the entire world".[11] Thereby, while small states may be subject to significant limitations in terms of resources and structural constraints (e.g. not being permanent members of the United Nations Security Council (UNSC)), it can be argued that they are nevertheless well positioned to play a modest though normatively critical role in defending international law.[12]

> *Cooperation and multilateral venues are of high importance to small states, who may use their strong position in such fora to feed into bilateral relationships*

Cooperation and multilateral venues are of high importance to small states, who may use their strong position in such fora to feed into bilateral relationships. However, in order to have an influence on the decisions of larger state actors, small states need to earn their counterparts' trust, prove to be stable and credible partners, and demonstrate solid diplomatic skills. In fact, politicians and diplomats from small states have the potential to establish a neutral standing and thereby serve as remarkably successful mediators, primarily by mastering the skill of searching for compromise.[13] On the

[9] United Nations General Assembly, "Developments in the Field of Information and Telecommunications in the Context of International Security: Report of the First Committee" (A/73/505), Seventy-third session, Agenda item 96, 19 November 2018, https://undocs.org/A/73/505; Ilona Stadnik, "Discussing State Behaviour in Cyberspace: What Should We Expect?" DiploFoundation, 20 March 2019, https://www.diplomacy.edu/blog/discussing-state-behaviour-cyberspace-what-should-we-expect.

[10] Mälksoo and Lupel, "A Necessary Voice".

[11] Mälksoo and Lupel, "A Necessary Voice".

[12] Mälksoo and Lupel, "A Necessary Voice".

[13] Liina Areng, *Lilliputian States in Digital Affairs and Cyber Security* (Tallinn Paper No. 4) (Tallinn: NATO CCDCOE, 2014), 4, https://ccdcoe.org/uploads/2018/10/TP_04.pdf.

other hand, small states are often reliant on like-minded coalitions or security alliances, and thereby may not be perceived as truly neutral in situations of clearly opposing debates.[14]

Small states may also successfully act as norm entrepreneurs. According to Martha Finnemore and Duncan Hollis, norms may arise in many ways:

> They may emerge spontaneously or through the entrepreneurship of one or more actors who frame the issue, articulate the norm, and organize support. If such efforts are successful, the norm may reach a tipping point and cause a "cascade" of norm adoption or, in other cases, cycles of norm change. Norm promoters draw on a variety of tools to construct the norm and create support for it, including incentives, persuasion, and socialization.[15]

Accordingly, norm entrepreneurs may be organisations, companies, individuals and states. They are critical to establishing a norm not only because they call attention to an issue in general but because they frame it. This entails employing language that names, interprets and dramatises the problem, and on that basis proposes a norm to address it, often also providing for an organisational platform.[16] And even if not qualifying as a norm entrepreneur as outlined by Martha Finnemore and Kathryn Sikkink's original research, studies have shown that, for small states with big ideas, the promotion of norms can be a powerful means to further national interests on the global level.[17]

2. Estonia as a Norm Promoter in Cybersecurity

As a digitally highly advanced society, Estonia has been at the forefront of discussions on cybersecurity since it was the target of the world's first coordinated cyber-attack campaign against a nation-state in 2007. This incident gave a boost to conceptualising cybersecurity on a domestic level (such as adopting the first cybersecurity strategy in 2008) as well as bringing the topic of cyber threats and the role of international cooperation in responding to such attacks to the agendas of international organisations such as NATO. Today, Estonia ranks high in global cybersecurity, Internet freedom and e-governance indexes.[18] The country also hosts relevant international organisations, such as the NATO Cooperative Cyber Defence Centre of Excellence (NATO CCDCOE, also the birthplace of the Tallinn Manual, and a number of globally well-known cyber exercises such as Locked Shields) and the EU Agency for Large-Scale IT Systems, and seeks to offer an innovative and supportive environment to start-ups and technology companies.

Estonia has played an important role in building and promoting cyber norms in international and regional fora

Estonia has played an important role in building and promoting cyber norms in international and regional fora. It has been an active member of the UN GGE on Developments in the Field of Information and Telecommunications in the Context of International Security in 2009–10, 2012–13, 2014–15, 2016–17 and 2019–21. Importantly, the UN GGE's landmark consensus report in 2013 affirmed the application of

[14] Liisi Adamson, "Let Them Roar: Small States as Cyber Norm Entrepreneurs," *European Foreign Affairs Review* 24, no. 2 (May 2019): 222, https://kluwerlawonline.com/journalarticle/European+Foreign+Affairs+Review/24.2/EERR2019014.

[15] Martha Finnemore and Duncan B. Hollis, "Constructing Norms for Global Cybersecurity," *American Journal of International Law* 110, no. 3 (July 2016): 445, https://doi.org/10.1017/S0002930000016894.

[16] Finnemore and Hollis, "Constructing Norms," 447–48.

[17] Martha Finnemore and Kathryn Sikkink, "International Norm Dynamics and Political Change," *International Organization* 52, no. 4 (1998): 887–917; Matthew Crandall and Collin Allan, "Small States and Big Ideas: Estonia's Battle for Cybersecurity Norms," *Contemporary Security Policy* 36, no. 2 (May 2015): 346–68, https://doi.org/10.1080/13523260.2015.1061765.

[18] "NCSI: Ranking," e-Governance Academy Foundation, accessed 7 February 2021, https://ncsi.ega.ee/ncsi-index/; Freedom House, *Freedom on the Net 2020: The Pandemic's Digital Shadow* (Washington, DC: Freedom House, 2020) https://freedomhouse.org/sites/default/files/2020-10/10122020_FOTN2020_Complete_Report_FINAL.pdf; United Nations Department of Economic and Social Affairs, *United Nations E-Government Survey: Digital Government in the Decade of Action for Sustainable Development* (New York, NY: United Nations, 2020), https://publicadministration.un.org/egovkb/Portals/egovkb/Documents/un/2020-Survey/2020%20UN%20E-Government%20Survey%20(Full%20Report).pdf.

international law in cyberspace, and the 2015 report proposed 11 norms for behaviour by states in cyberspace. In 2019–21 Estonia is also a member of the UN OEWG. While both the UN GGE and the OEWG are political discussions and not law-making processes per se, they have a significant role to play in shaping and establishing international agreement on norms of behaviour in cyberspace. In addition to global platforms, Estonia values the role of regional organisations in building trust and confidence between states and enforcing agreed norms.[19]

Estonia and other co-hosting countries put cybersecurity on the agenda of the UNSC, which had never before discussed the subject

As a major contribution, Estonia and other co-hosting countries put cybersecurity on the agenda of the UNSC, which had never before discussed the subject. As part of Estonia's Presidency of the UNSC, it organised an Arria-formula meeting focusing on cyber stability, conflict prevention and capacity building. Around 60 countries and organisations took part, many stressing the application of international law in cyberspace and underlining that norms of responsible state behaviour hold for all UN member states.[20] In addition, Estonia, supported by the UK and the US, raised the issue of responsible state behaviour in cyberspace in the UNSC and issued a joint stakeout condemning a large-scale cyber-attack conducted by Russia's military intelligence service against the government and media websites in Georgia in October 2019.[21]

These steps illustrated how active participation in international organisations allows small nations to bring urgent issues such as cybersecurity into the global limelight.

As a concrete step towards more clarity over the interpretation of international law, Estonia delivered its views on the issue in 2019. President Kersti Kaljulaid underlined in her speech the protection provided by international law to small states, stating that Estonia did not have "the luxury" of remaining unambiguous about the meaning of legal norms in cyberspace, and invited other nations to call out cyber operations that constitute a violation of international law.[22] The Estonian position includes several important points on due diligence and the right to resort to countermeasures. While its stance did not entail a clarification on the issue of whether sovereignty is a stand-alone rule or principle in international law, Estonia made a bold statement on collective response to malicious cyber activities, stating that "states which are not directly injured may apply countermeasures to support the state directly affected by the malicious cyber operation". It was the first country in the world to offer such an interpretation of international law.[23]

Estonia made a bold statement on collective response to malicious cyber activities, stating that "states which are not directly injured may apply countermeasures to support the state directly affected by the malicious cyber operation". It was the first country in the world to offer such an interpretation of international law

While the majority of other countries have not expressed their opinion about collective countermeasures, the proposal has certainly

[19] Permanent Mission of Estonia to the UN, "Opening Statement by the Republic of Estonia, by Amb. Heli Tiirmaa-Klaar for the UN GGE Panel on Regional Consultations," 2019, https://www.un.org/disarmament/wp-content/uploads/2019/12/estonia-gge-panel-on-regional-consultations-05-12-2019.pdf.

[20] Permanent Mission of Estonia to the UN, "At Estonia's Initiative, the International Community Reaffirmed the Importance of Cyber Stability, Including during the COVID-19 Crisis, at the UN Security Council," 23 May 2020, https://un.mfa.ee/at-estonias-initiative-the-international-community-reaffirmed-the-importance-of-cyber-stability-including-during-the-covid-19-crisis-at-the-un-security-council/.

[21] Permanent Mission of Estonia to the UN, "Stakeout on Cyber-Attack against Georgia by Estonia, the United Kingdom and the United States," 5 March 2020, https://un.mfa.ee/press-stakeout-by-estonia-the-united-kingdom-and-the-united-states-on-cyber-attack-against-georgia/.

[22] Office of the President of Estonia, "Speech of the President of the Republic of Estonia at the Opening of CyCon 2019," 29 May 2019, https://www.president.ee/en/official-duties/speeches/15241-president-of-the-republic-at-the-opening-of-cycon-2019/index.html.

[23] Michael Schmitt, "Estonia Speaks Out on Key Rules for Cyberspace," Just Security, 10 June 2019, https://www.justsecurity.org/64490/estonia-speaks-out-on-key-rules-for-cyberspace/.

drawn attention to the need to review states' options for responding to malicious cyber activities. Moreover, the proposal signals to wrong-doers that the consequences of attacking a small state need not be limited to that state's own capabilities. So far, France has rejected the concept of collective countermeasures, while New Zealand acknowledges their possible use in assisting victim states in applying proportionate countermeasures to induce compliance by the state acting in breach of international law.[24] If Estonia decides to promote this norm internationally by framing the issue, further articulating the need and reasoning, and organises support from other countries, it could be seen as a norm entrepreneur as prescribed by Finnemore and Sikkink.

Also relevant is Estonia's role in raising awareness and providing training on different aspects of state behaviour in cyberspace. In addition to the wide range of training provided by the NATO CCDCOE, the Estonian Ministry of Foreign Affairs has organised high-level summer and winter schools for diplomats across the world. Equally, the Estonian Information System Authority is the coordinating body for the EU-wide network of cybersecurity experts CyberNet and a partner of the EU's Cyber for Development Project (Cyber4Dev), which aims to support the enhancement of cybersecurity in Africa, Asia, Latin America and the Caribbean through various training programmes. [25]

Given the above, it is fair to conclude that Estonia's continuous activity targeting different facets of cybersecurity and norms for responsible state behaviour, promoting cyber stability and cooperation, and acting as a trustworthy partner and trainer, has over time cultivated for the small country a reputation for consistency and credibility in the domain of cybersecurity and norms of state behaviour in cyberspace.

3. Estonia and Japan Fostering Cooperation in Cybersecurity

Estonia and Japan have many similarities in their approach to state behaviour in cyberspace, which has established firm ground for closer bilateral ties. Both face complicated geopolitical challenges and both are active members in international and regional organisations dealing with norms in cyberspace. As leaders in cyber diplomacy, they frequently speak out on the applicability of international law to cyberspace, and express concerns about states carrying out malicious cyber operations. Importantly, Estonia and Japan play an active part in negotiations in the UN GGE and OEWG, where their main positions largely converge. These include: (1) views on the applicability of international law, (2) the lack of a need for a new legally binding instrument on cybersecurity, (3) relevance on implementation of already agreed norms, and (4) the centrality of confidence and capacity building. While Estonia has submitted its views for inclusion in an annex to UN GGE reports on one occasion (in 2017), Japan has been more active and shared its domestic views three times (in 2016, 2017 and 2019).[26]

> *Estonia and Japan have many similarities in their approach to state behaviour in cyberspace, which has established firm ground for closer bilateral ties*

[24] Ministère des Armées (Ministry of Armed Forces), *Droit International Appliqué Aux Opérations Dans Le Cyberspace* [International Law Applied to Cyberspace Operations] (Paris: Délégation à l'information et à la communication de la défense, 2019), 8, https://www.defense.gouv.fr/content/download/565895/9750877/file/Droit+internat+appliqu%C3%A9+aux+op%C3%A9rations+Cyberespace.pdf; Ministry of Foreign Affairs and Trade of New Zealand, "The Application of International Law to State Activity in Cyberspace," 1 December 2020, para. 22, https://dpmc.govt.nz/sites/default/files/2020-12/The%20Application%20of%20International%20Law%20to%20State%20Activity%20in%20Cyberspace.pdf.

[25] "EU CyberNet – the bridge to cybersecurity expertise in the European Union," EU CyberNet, last accessed 18 February 2021, https://www.eucybernet.eu/; "We are Cyber 4 Dev," Cyber4DEV, last accessed 18 February 2021, https://cyber4dev.eu/.

[26] United Nations Office for Disarmament Affairs, "2017 Submissions from Member States: Estonia – Response to the General Assembly Resolution 70/237 on 'Developments in the Field of Information and Telecommunications in the Context of International Security'," 2017, https://unoda-web.s3.amazonaws.com/wp-content/uploads/2017/09/Estonia-full.pdf; United Nations Office for Disarmament Affairs, "2016 Submissions from Member States: Japan," 2016, https://unoda-web.s3-accelerate.amazonaws.com/wp-content/uploads/2016/10/Japan.pdf; United Nations Office for Disarmament Affairs, "2017 Submissions from Member States: Japan,"2017, https://unoda-web.s3.amazonaws.com/wp-content/uploads/2017/09/Japan.pdf; United Nations Office for Disarmament Affairs, "2019 Submissions from Member States: National Reply from Japan," 2019, https://unoda-web.s3.amazonaws.com/wp-content/uploads/2019/09/Japan-2019.pdf.

The alignment of values and principles between the two countries can also be seen in a number of other initiatives. For example, Estonia and Japan joined the statement on advancing responsible state behaviour, which promises to hold states accountable for actions breaching international law.[27] Estonia and Japan are also both signatories of the recent proposal for the Programme of Action to Advance Responsible State Behaviour in Cyberspace, which focuses on continuing institutional dialogue within the UN and moving forward with implementing the already agreed norms.[28] In addition, the two countries' support for each other's endeavours was outlined in a speech by the UN High Representative for Disarmament, Izumi Nakamitsu, delivered at the opening of a cyber event organised by Estonia in the margins of the UNSC.[29] It is also noteworthy that Estonia and Japan are among the signatories of the Council of Europe Convention on Cybercrime, and thereby actively promoting the expansion of its parties, strengthening international cooperation among law-enforcement authorities, assuring prompt and effective assistance in investigation, and facilitating international investigations.

On an institutional level, the two countries have cooperated over various aspects of cybersecurity since 2014, having signed a Memorandum of Understanding in 2015. Bilaterally, national views and best practices have been exchanged on a number of issues regarding technical capabilities, training and domestic frameworks. Japan contributed to the NATO CCDCOE as an observer in 2015–18 and joined as a Contributing Participant in 2019.

> *Both countries should continue efforts to raise awareness on responsible state behaviour in cyberspace*

Conclusions

In future work, it is hoped that Estonia and Japan will identify further options for practical cooperation within the domain of cyber norms, and continue to develop their collaboration in technical, training, policy and other areas. Specifically, both countries should continue efforts to raise awareness on responsible state behaviour in cyberspace. General capacity building and information sharing on international law and its characteristics will be essential to reach a wider agreement on a number of issues related to norms. These include: (1) the long-lasting debate on the need for new norms as opposed to focusing on the implementation of existing ones, (2) different views on balancing sovereign rights and international commitments, and (3) the applicability of international humanitarian law to the militarisation of cyberspace.

> *Estonia and Japan should continue to identify and share their domestic views, legal assessments and experience related to cybersecurity*

Equally, Estonia and Japan should continue to identify and share their domestic views, legal assessments and experience related to cybersecurity. Sharing information on the threat landscape and experience in mitigating cyber incidents will also be highly beneficial. As role models, the countries have the potential to influence other states in their respective regions to be more transparent regarding state practice and cooperation in terms of finding common ground in discussing norms, and in collaboration of a more technical nature.

[27] US Department of State Office of the Coordinator for Cyber Issues, "Joint Statement on Advancing Responsible State Behavior in Cyberspace," 23 September 2019, https://www.state.gov/joint-statement-on-advancing-responsible-state-behavior-in-cyberspace/.

[28] United Nations Office for Disarmament Affairs, "The Future of Discussions on ICTs and Cyberspace at the UN (Submission by France, Egypt, Argentina, Colombia, Ecuador, Gabon, Georgia, Japan, Morocco, Norway, Salvador, Singapore, the Republic of Korea, the Republic of Moldova, The Republic of North Macedonia, the United Kingdom, the EU and its member States – Austria, Belgium, Bulgaria, Croatia, Republic of Cyprus, Czech Republic, Denmark, Estonia, France, Finland, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain and Sweden)," 8 October 2020, https://front.un-arm.org/wp-content/uploads/2020/10/joint-contribution-poa-future-of-cyber-discussions-at-un-10-08-2020.pdf.

[29] United Nations Office for Disarmament Affairs, "Briefing at the Security Council Virtual Arria-Formula Meeting on 'Cyber Stability, Conflict Prevention and Capacity Building': Remarks by Ms. Izumi Nakamitsu, High Representative for Disarmament Affairs," 22 May 2020, https://front.un-arm.org/wp-content/uploads/2020/05/UNSC-Arria-Formula-Meeting-on-Cybersecurity-HR-Remarks-22-May-2020.pdf.

As active members of regional organisations such as the EU and Asia-Pacific Economic Cooperation (APEC), Estonia and Japan also have the opportunity to guide discussion and serve as the voice of their closest neighbours and partners. For example, the EU is already taking concrete steps in finding a common voice for its 27 members by proposing to develop a joint position on the application of international law in cyberspace.[30]

Estonia and Japan may be far apart in geographical terms, but they are close in their understanding of the role, scope and objective of building norms in cyberspace

Estonia and Japan may be far apart in geographical terms, but they are close in their understanding of the role, scope and objective of building norms in cyberspace. The constructive cooperation and broad agreement on the future of the institutional setting for facilitating the international discussion on norms, international law, confidence building and capacity building are proof of common values. The close relationship between Estonia and Japan serves as an example of how the small size and population of a country has no effect on its credibility as an ally in promoting and developing norms of state behaviour in cyberspace.

[30] European Commission, *The EU's Cybersecurity Strategy for the Digital Decade*.