Legal instability in cyberspace and OSCE's mitigation role

Postdoctoral researcher **Adina PONTA**[1]

Abstract

After the international legal community widely endorsed the application of international law to cyberspace, many open questions remain on the concrete interpretation of existing rights and obligations to the cyber realm. In pursuit of its mandate to promote human rights and conflict prevention, the OSCE can play a major role to support operationalization of international law and application of existing principles to cyberspace. This paper examines some key steps in the aftermath of the creation of norms of behavior, and transparency and confidence-building measures. After a brief analysis of the norm-creation process, this piece identifies several pressing cybersecurity challenges on the international landscape, and offers suggestions for consolidating the voluntary non-binding norms States agreed upon. Using lessons learned from other domains, the analysis will focus on mechanisms of building further stability and transparency in cyberspace, in particular by reference to the due diligence principle and States' human rights obligations.

Keywords: *confidence-building measures, norms of behavior, due diligence, cybersecurity, OSCE.*

JEL Classification: K24, K33

DOI: 10.24818/TBJ/2021/11/3.01

1. Introduction

Increased use of technology in civil, military, and commercial sectors, and associated threats have forced scholars and States to consider the international law implications of this new reality. After States, international organizations, and international coordinating fora endorsed the application of international law to cyberspace, the debate shifted to questions of how existing principles, rights, and obligations should be interpreted in the cyber realm.[2] Various exercises have

[1] Adina Ponta - Faculty of Law, Babeș-Bolyai University in Cluj-Napoca, Center for Business Law & Information Technology, Romania, ponta.adina@gmail.com.

[2] For e.g., "Cybersecurity Strategy. Republic of Estonia 2019-2022," *Ministry of Economic Affairs and Communications,* February 2018, https://www.mkm.ee/sites/default/files/kyberturvalisuse strateegia_2022_eng.pdf; "Strategic Review of Cyber Defence," *Repulique Francaise - Secrétariat Général de la Défense et de la Sécurité Nationale,* February 2018, http://www.sgdsn.gouv.fr/uploads/2018/03/revue-cyber-resume-in-english.pdf; "Dutch National Cyber Security Agenda," *The Netherlands' Ministry of Justice and Security*, April 2018, https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/national-cyber-security-strategy-1; "The UK National Cyber Security Strategy 2016-2021," *HM Government*, 2016, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/natio nal_cyber_security_strategy_2016.pdf; "National Cyber Strategy of the United States of America," *The White House*, September 2018,

attempted to identify the applicable international rules, possible State responses, and legal consequences of cyberoperations, both during war and during peacetime.

States quickly realized that national security heavily depends on international cooperation. International efforts to counter cybersecurity risks debuted with Russia's introduction of a first United Nations (U.N.) resolution on this topic in 1998.[3] Numerous cyber policy fora have proliferated since then in diverse formats, such as the U.N. Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (GGE), the subsequent U.N. Open-Ended Working Group on Developments in the Field of ICTs in the Context of International Security (OEWG), and other industry-focused norm processes.[4] These multistakeholder initiatives started to shape cooperative tools, norms of behavior, and confidence-building measures (CBMs) in support of collective cybersecurity. One of the exercises which is regarded among the most successful by the international community is the high-level agreement on principles, norms, and rules of the road for national internet activities and transnational cyber interactions, conducted under the auspices of the Organization for Cooperation and Security in Europe (OSCE).

In pursuit of its mandate to promote human rights and conflict prevention, the OSCE can play a major role to support operationalization of international law and application of existing principles to the cyber realm. This paper examines some key steps for the aftermath of the creation of norms of behavior, and transparency and confidence-building measures (TCBMs). After a brief analysis of norm-creation processes (part II), this paper will identify some of the most pressing cybersecurity challenges on the international landscape (part III), and offer some suggestions for consolidating the voluntary non-binding norms States already agreed upon (part IV). Using the lessons learned from other domains, the analysis will focus on mechanisms of building further stability and transparency in cyberspace, in particular by reference to the due diligence principle and States' human rights obligations.

---

https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf; "Declaration by the High Representative Josep Borrell, on behalf of the E.U., on malicious cyber activities exploiting the coronavirus pandemic," *Press Release* 26/120, April 30, 2020, https://www.consilium.europa.eu/en/press/press-releases/2020/04/30/declaration-by-the-high-representative-josep-borrell-on-behalf-of-the-european-union-on-malicious-cyber-activities-exploiting-the-coronavirus-pandemic/; "G-8 Declaration Renewed Commitment For Freedom and Democracy," *G-8 Summit Deauville*, May 2011, https://www.nato.int/nato_static/assets/pdf/pdf_2011 _05/20110926_110526-G8-Summit-Deauville.pdf. [all accessed 15.06.2021].

[3] Theresa Hitchens and Nancy W. Gallagher, "Building Confidence in the Cybersphere: A Path to Multilateral Progress," *Journal of Cyber Policy* 4, no. 1 (2011): 4, https://doi.org/10.1080/23738871.2019.1599032. [accessed 15.06.2021].

[4] For e.g., "Stay Smart. Stay Safely Connected," *Cybersecurity Tech Accord*, May 13, 2020, https://cybertechaccord.org/; "Global Conference on Cyber Space (GCCS) 2017," *Internet Society*, November 23-24, 2017, https://www.internetsociety.org/events/gccs-2017/; "The 9 Principles," Paris Call, December 11, 2018, https://pariscall.international/en/supporters [all accessed 15.06.2021].

2. From norm creation to consolidation

Analysis of traditional Areas Beyond National Jurisdiction can provide useful lessons learned for cyberspace and demonstrates that if States desire, global governance is possible, even in domains not covered by territorial sovereignty, such as outer space, the High Seas, and Antarctica.[5] The traditional power race is reflected in cyberspace, and this domain reveals additional challenges for reaching a multilateral agreement, including lack of consensus on defining fundamental legal terms and interpretations of internal and external State sovereignty.[6]

While most States seem to agree on the application of general international law to transboundary cyberoperations, the precise translation of the rules developed in the physical world to cyberspace is widely debated. If States see a need to develop new rules, these should build on and strengthen the existing legal framework. The creation of international cybernorms is at the States' discretion, as it is these international law actors that will be bound by any new rules. Efforts such as that which produced the Tallinn Manuals can play extremely valuable roles, but are no substitute for State practice or articulation of norms. On the one hand, these exercises provide an opportunity for a thorough understanding of normative expectations within relevant communities. On the other hand, they have fragmented the legal approach to cyberspace, which further hampers cybernorms ability to solidify and diffuse. Fragmentation is most visible with respect to the scope of notions such as the threshold of the use of force, due diligence, and essential State infrastructure, all which will be detailed below.[7]

Additionally, most norm-making fora focus on the end product, i.e., the creation of norms and their substantive content. The process itself is often understated, although it represents the catalysator of building trust and understanding, and the real power of a successful future of norms lies in the processes by which they form and evolve. Therefore, it was argued that the journey matters as much as the destination, namely the manner in which cybernorms are constructed will shape the content and character of the emerging norms.[8]

Norms are voluntary forms of cooperation, usually framed in a general language, that provide ideal standards of conduct for State and non-State actors. Usually lacking compliance, enforcement, and dispute resolution mechanisms, their value derives from implementation and careful balancing of additional State commitments, national security considerations, privacy concerns, and private-public partnerships. Although cybernorms discourse has often focused on promoting

---

[5] Kristen Eichensehr, "The Cyber-Law of Nations," *Georgetown Law Journal* 103, no. 2 (2015): 317.

[6] Christian Ruhl et al., "Cyberspace and Geopolitics: Assessing Global Cybersecurity Norm Processes at a Crossroads," *Carnegie Endowment for International Peace Working Paper* (2020): 16, https://carnegieendowment.org/files/Cyberspace_and_Geopolitics. pdf., [accessed 15.06.2021].

[7] Adina Ponta, "Cyber Operations Against Medical Facilities During Peacetime*," Lawfare Blog,* May 1, 2020, https://www.law fareblog.com/cyber-operations-against-medical-facilities-during-peacetime. [accessed 15.06.2021].

[8] Martha Finnemore and Duncan B. Hollis, "Constructing Norms for Global Cybersecurity," *American Journal of International Law* 110, no. 3 (2016): 429.

voluntary non-binding norms as an alternative to law, legal rules and norms are not antagonistic concepts. The goal of law creation is precisely the establishment of norms, and their legitimacy is conferred by creation of collective behavioral expectations. Most existing cybernorms are built on bases other than law, such as political agreement.[9] Some of these multi-stakeholder efforts were intended to be as inclusive as possible, campaigning for universal cybernorms for all States.[10] Other initiatives targeted limited norm development, addressing "like-minded States", "major powers" or specific domains, such as data protection.[11] The most known multilateral norm-building efforts in cyberspace are the GGE process and the OSCE efforts to develop voluntary CBMs.

TCBMs are policy tools aimed at mitigating threats, building trust, and communication channels, and have been traditionally promoted in tackling international security issues, such as nuclear non-proliferation or disarmament. Usually perceived as politically binding instruments, TCBMs can sometimes be agreed as legally binding, but they are mainly constructed as a bridge to future international law rules, laying the foundations towards identification of areas of common ground.[12] Flexibility and openness to understand perspectives of allies and competitors is both a crucial condition and an aim of efficient TCBMs, as was demonstrated by the CBMs agreed under the umbrella of the OSCE.[13]

Even in the ideal case of norm formation and internalization among target groups, compliance is a continuous process. Each application represents a further interpretation and development exercise, adding a new layer of shared understanding to the norm substance. Each time stakeholders make a conscious decision regarding the meaning and requirement implied by a norm in a particular context, they shape collective expectations about appropriate behaviors.

---

[9] This is the case for the G-20 endorsement of prohibition on cyberespionage for commercial purposes, the OSCE Parliamentary Declaration & Resolution on Cybersecurity, and the Shanghai Cooperation Organization's Code of Conduct for Information Security. "G-20 Leaders' Communique´," *Antalya Summit*, November 15–16, 2015, para. 26, http://www.mofa.go.jp/files/000111117.pdf; "2013 Istanbul Final Declaration and Resolution on Cyber Security," *OSCE Parliamentary Assembly*, June 29-July 3, 2013, https:// www.oscepa.org/meetings/annual-sessions/2013-istanbul-annual-session/2013-istanbul-final-declaration/1652-15; "U.N. Document A/69/723, International Code of Conduct for Information Security", in *Letter from the Permanent Representatives of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan to the United Nations Secretary-General,* January 9, 2015, https://digitallibrary.un.org/record/786846/files/A_69_723-EN.pdf. [all accessed 15.06.2021].

[10] For e.g. the "U.N. General Assembly, Resolution 73/266, Advancing Responsible State Behaviour in Cyberspace in the Context of International Security", A/RES/73/266, December 22, 2018, https://undocs.org/pdf?symbol=en/A/RES/73/266; "London Process", formally called "Global Conference on Cyber Space", Global Forum on Cyber Expertise, https://www.thegfce.com/about/gccs; [accessed 15.06.2021].

[11] For e.g., the two international Codes of Conduct for information security developed by the Shanghai Cooperation Organization, the Budapest Convention on Cybercrime sponsored by the Council of Europe, the Tallinn Manuals developed under the auspices of NATO Cooperative Cyber Defence Centre of Excellence (CCD CoE). See *infra*15.

[12] Ben Baseley-Walker, "Transparency and Confidence-Building Measures in Cyberspace: Towards Norms of Behaviour," *Confronting Cyberconflict* (2011): 33, https://citizenlab.ca/cybernorms2012/BaseleyWalker2011.pdf. [accessed 15.06.2021].

[13] Baseley-Walker, "Transparency and Confidence-Building," 32.

3. The role of due diligence in creating stability

3.1 Cyber Due Diligence

This paper identified a number of imminent themes which merit some discussion at the outset, the most relevant being closely related to the application of the principle of sovereignty. The international community is divided on the legal qualification of sovereignty, i.e., whether it represents a principle or a rule of international law.[14] Nevertheless, it is accepted that in cyberspace, sovereignty reflects States' exclusive legal authority over their cyber infrastructure and activity associated with it.[15] Deriving due diligence duties in cyberspace from the principle of equal State sovereignty, Rule 6 of the Tallinn Manual 2.0. notes States' obligation to ensure that the territory or cyber infrastructure under their control is not used for operations that affect the rights of, and produce adverse consequences for, other States.[16]

Although in the environmental law context, due diligence has been recognized as a principle of customary international law, it has no binding nature in the cyber realm.[17] The uncertain scope of this obligation and consequences of non-compliance were echoed by the 2015 GGE report.[18] This imprecise language might reflect the lack of States' endorsement of the customary international law character of the due diligence duty.[19] In contrast to the generic wording used by

[14] Gary P. Corn and Robert Taylor, "Sovereignty in the Age of Cyber," *American Journal of International Law Unbound* 111 (2017): 208, doi:10.1017/aju.2017.57; Michael N. Schmitt and Liis Vihul, "Respect for Sovereignty in Cyberspace," *Texas Law Review* 95, no. 7 (2017):1639; Harriet Moynihan, "The Application of International Law to State Cyberattacks: Sovereignty and Non-Intervention," *Chatham House Research Paper* (2019):8, https://www.chathamhouse.org/sites/default/files/publications/research/20 19-11-29-Intl-Law-Cyberattacks.pdf. [accessed 15.06.2021].

[15] Eric T. Jensen, "The Tallinn Manual 2.0: Highlights and Insights," *Georgetown Journal of International Law* 48 (2017): 735; Scott J. Shackelford et al., "Unpacking the International Law on Cybersecurity Due Diligence: Lessons from the Public and Private Sectors," *Chicago Journal of International Law* 17, no.1 (2016): 1.

[16] Michael N. Schmitt, ed., *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge: Cambridge University Press, 2017). The Tallinn Manual 2.0 is an influential resource for lawyers who advise on international law applicable to cyberspace, produced by an international group of legal scholars and practitioners at the invitation of the Tallinn-based NATO CCD CoE; Adina Ponta, "Security and Human Rights Challenges of Cyber Due Diligence," *Harvard International Law Journal Online* (2020), https://harvardilj.org/2020/06/security-and-human-rights-challenges-of-cyber-due-diligence/. [accessed 15.06.2021].

[17] Peter Z. Stockburger, "From Grey Zone to Customary International Law: How Adopting the Precautionary Principle May Help Crystallize the Due Diligence Principle in Cyberspace," in *NATO CCD CoE Publications*, eds. T. Minárik, R. Jakschis, and L. Lindström (Talinn, 2018), 250; International Court of Justine (ICJ) Judgement *Certain Activities Carried Out By Nicaragua In The Border Area (Costa Rica V. Nicaragua),* December 16, 2015.

[18] "U.N. Document A/70/174, Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security," July 22, 2015, https://undocs.org/A/70/174 [hereinafter GGE 2015 report]. [accessed 15.06.2021].

[19] The rejection of a mandatory due diligence rule within the GGE, which might as well represent valid *opinio juris*, mainly underlies fears of burdensome oversight obligations such a rule would impose on States with massive technological capabilities; Permanent Court of Arbitration, *Trail Smelter*

international fora, individual States often address due diligence in granular statements.[20] There is however no consensus on the content of the due diligence obligation, nor on whether this duty also entails a preventive aspect, which in case of violation would constitute an internationally wrongful act.[21] Prevention, the procedural component of due diligence, has been endorsed in various international instruments from other areas of law and by international organizations.[22]

Due diligence is an objective principle of law, but the assessment of compliance represents a sliding scale based on different factors, such as knowledge, capabilities, risks, and consequences. As such, the assessment of whether the expected vigilance was met, is variable and flexible.[23] A major challenge to create an enforceable international law obligation with a preventive component is the existence of different economic and technological State capabilities, although the fundamentals and standards of State responsibilities are common.[24]

Case (*United States v. Canada*), *U.N. Reports of International Arbitral Awards,* 2006, https://legal.un.org/riaa/cases/vol_III/1905-1982.pdf; Michael N. Schmitt, "Grey Zones in the International Law of Cyberspace," *The Yale Journal of International Law Online* 42, no. 2 (2017): 15.

[20] This also translates into acceptance of the consequences of internationally wrongful acts, such as political or diplomatic actions, including those implemented via the U.N. Security Council. Michael Schmitt, "The Netherlands Releases a Tour de Force on International Law in Cyberspace: Analysis", *Just Security*, October 14, 2019, https://www.justsecurity.org/66562/the-netherlands-releases-a-tour-de-force-on-international-law-in-cyberspace-analysis/. For individual states' declarations, see Przemyslaw Roguski, "Application of International Law to Cyber Operations: A Comparative Analysis of States' Views," *The Hague Program for Cyber Norms Policy brief,* March 2020, https://www.thehaguecybernorms.nl/research-and-publication-posts/application-of-international-law-to-cyber-operations-a-comparative-analysis-of-states-views. [accessed 15.06.2021]

[21] "GGE 2015 report", note 18 above. According to the International Law Commission (ILC), States are expected to employ vigilance on their territory, a duty that has developed in relation to their responsibility for private activities; "Annex to General Assembly resolution 56/83 of December 12, 2001 and corrected by document A/56/49(Vol. I)/Corr.4." Responsibility of States for Internationally Wrongful Acts, 2001, https://legal.un.org/ilc/texts/instruments/english/draft_articles/9_6_2001.pdf [hereinafter ILC Draft Articles]; Karine Bannelier and Theodore Christakis, "Cyber-Attacks – Prevention-Reactions: The Role of States and Private Actors," *Les Cahiers de la Revue Défense Nationale*, (February 2017):19.

[22] For e.g. the European Union (EU), the World Trade Organization (WTO), the International Tribunal for the Law of the Sea (ITLOS), and, in the environmental context, the ICJ. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, *Official Journal of the European Union*, L 119/1 (April 27, 2016), called "GDPR"; ITLOS Request for Advisory Opinion submitted to the Seabed Disputes Chamber, *Responsibilities and Obligations of States Sponsoring Persons and Entities with Respect to Activities in the Area*, February 1, 2011; ICJ Judgement in *Case Concerning Pulp Mills on the River Uruguay (Argentina v. Uruguay),* April 20, 2010. By analogy with international environmental law, States would have to assess cyber activities within their jurisdiction, similar to the obligation to conduct an environmental impact assessment, when there is a likelihood that transboundary harm would occur from these activities. Stockburger, "From Grey Zone to Customary International Law," 252.

[23] "Laws of gravitation. Due diligence obligations in cyberspace," in *EU Cyber Sanctions and Norms in Cyberspace*, eds. Patryk Pawlak and Thomas Biersteker (Chaillot Paper 155), October 2019, https://www.iss.europa.eu/sites/default/files/EUISSFiles/cp155.pdf. [accessed 15.06.2021].

[24] While the Estonian President implied the existence of preventive obligations on States, she included the development of assistive means to support target States in the attribution and investigation of

3.2 Due Diligence and Intersections with Human Rights Law

States' obligations to safeguard human rights apply (1) in relation to individuals located on their territory, and (2) to obligations under international law to prevent transboundary harm. Although application of international human rights law (IHRL) to cyberspace is widely recognized, the majority of States don't regard the geographic scope of human rights treaty obligations as being "extraterritorial," and consider themselves to have affirmative obligations to prevent and respond to human rights violations only on their territory.[25] Transboundary obligations arise when a State exercises real or *de facto* control and authority over a territory.[26]

Temporal and spatial applicability of state sovereignty and associated jurisdiction is more complex in a domain that lacks physical territory and exclusive effective control.[27] During the 2020 pandemic, the complexity of establishing States' responsibility in relation to the individuals who were injured or could have lost their lives as a consequence of a preventable hostile cyberoperation, became evident.[28] In this context, in relation to their own citizens, States' obligations to provide cybersecurity will have to be integrated within the scope of the right to life, the right to health, and the right to freedom and security, in order to trigger the relevant reparation mechanisms provided by regional and international human rights instruments. The right to health is safeguarded by the International Covenant on Economic, Social and Cultural Rights (ICESCR), which some States have not ratified to date.

The theory that positive IHRL obligations, including a due care requirement, can and should arise under international law in extraterritorial circumstances has already been discussed in other contexts, especially related to international law

malicious activities in the scope of "reasonable efforts," depending on States' capacities. President Kersti Kaljulaid, "President of the Republic at the opening of CyCon 2019," May 29, 2019, https://www.president.ee/en/official-duties/speeches/15241-president-of-the-republic-at-the-opening-of-cycon-2019/index.html; "GGE 2015 report", note 18 above. Karine Bannelier, "Cyber Diligence: A Low-Intensity Due Diligence Principle for Low-Intensity Cyber Operations?," *Baltic Yearbook of International Law* 14 (2014):8.

[25] Monika Heupel, "How do States Perceive Extraterritorial Human Rights Obligations? Insights from the Universal Periodic Review," *Human Rights Quarterly* 40, no. 3 (2018): 522.

[26] Antal Berkes, "Human Rights Obligations of the Territorial State in the Cyberspace of Areas Outside Its Effective Control," *Israel Law Review* 52, no. 2 (2019): 210. The European Court of Human Rights (ECtHR) has recognized a certain degree of extraterritoriality when States operate abroad. The Tallinn Manual 2.0 has embraced the extraterritoriality standard of the Human Rights Committee within the power or effective control, which can be over territory (spatial model) or over individuals (personal model). Ido Kilovaty, "An Extraterritorial Human Right to Cybersecurity," *Notre Dame Journal of International and Comparative Law* 10, no.1 (2020): 44.

[27] Therefore, an exclusive focus on territoriality may undermine the ability to respect, protect, and fulfil human rights in cyberspace and the kind of power that States may exert over individuals online. *Id.,* 42.

[28] Ponta, "Cyber Operations," note 7 above.

applicable to the environment.[29] Human rights bodies have attached to the due diligence principle a duty to investigate and to prevent, extended by scholars to human rights violations in cyberspace.[30] However, the majority of scholars reject a general obligation of prevention.[31] Moreover, addressing the right to health, the U.N. Committee on Economic, Social, and Cultural Rights (CESCR) highlighted States' obligations to respect the enjoyment of the right to health in other countries.[32] This rationale implies that even if States do not recognize the application of the due diligence principle and its preventive component, their obligation to prevent transboundary harm, including the harm resulting from hostile cyberoperations on medical and testing facilities, could be derived from transboundary IHRL obligations, or the universality of human rights.

Reaching a balance between protection of individual rights and national security is a complex effort.[33] Fortunately, for the purpose of protecting their national security, most States would act with due diligence simply because it is in their domestic and foreign policy interest. The open question is of how to legally address transboundary human rights violations of hostile cyberoperations in the absence of a unitary approach on transboundary effects of States' human rights obligations and given the non-binding nature of due diligence. Customary international law, including parts of the International Law Commission's Draft Articles on the Responsibility of States for Internationally Wrongful Acts, might be the answer in case of unlawful and attributable State actions, although their application to the cyber

[29] Samantha Besson, "Due Diligence and Extraterritorial Human Rights Obligations – Mind the Gap!," *ESIL Reflections* 9, no. 1 (2020): 7, https://esil-sedi.eu/wp-content/uploads/2020/04/ESIL-Reflection-Besson-S.-3.pdf [accessed 15.06.2021].

[30] Berkes, "Human Rights Obligations," 212.

[31] "U.N. Document CCPR/C/21/Rev.1/Add. 1326, "International Covenant on Civil and Political Rights. General Comment No. 31," Human Rights Committee (HRC), May 2004, http://docstore.ohchr.org/SelfServices/FilesHandler.ashx?enc=6QkG1d%2FPPRiCAqhKb7yhsjYoiCfMKoIRv2FVaVzRkMjTnjRO%2Bfud3cPVrcM9YR0iW6Txaxgp3f9kUFpWoq%2FhW%2FTpKi2tPhZsbEJw%2FGeZRASjdFuuJQRnbJEaUhby31WiQPl2mLFDe6ZSwMMvmQGVHA%3D%3D [accessed 15.06.2021]; ECtHR Case *López Ostra v. Spain,* Application no. 16798/90 (2004).

[32] "International Covenant on Economic, Social and Cultural Rights," *adopted and opened for signature, ratification and accession December 16, 1966*, U.N.G.A Resolution 2200A (XXI) (entered into force Jan. 3, 1976), https://www.ohchr.org/en/professional interest/pages/cescr.aspx; "U.N. Document E/C.12/2000/4, CESCR General Comment No. 14: The Right to the Highest Attainable Standard of Health (Art. 12)," August, 11, 2000: "State parties [to the ICESCR] have to respect the enjoyment of the right to health in other countries." According to the Maastricht Principles, States should be held accountable for violating human rights of people outside of their own territories. "Maastricht Principles on the Extra-Territorial Obligations of States in the area of Economic, Social and Cultural Rights," September 28, 2011, https://www.ciel.org/wp-content/uploads/2015/05/Maastricht_ETO_Principles_21Oct11.pdf. [accessed 15.06.2021].

[33] ECtHR Case *Osman v. The United Kingdom,* no. 87/1997/871/1083, October 28, 1998: this positive obligation to take preventive operational measures shall "not impose an impossible or disproportionate burden on the authorities." Rule 36 of the Tallinn Manual 2.0. notes States' affirmative obligation to ensure respect for human rights and to protect human rights from abuse by third parties.

domain is sometimes disputed.[34] The importance of the due diligence principle cannot be overstated in the context of conflict prevention, and the same is valid for the value of trust-building for a successful common understanding of this international law principle.

4. The process of consolidating existing norms under the OSCE umbrella

4.1 The old and new role of the OSCE

The more we try to perceive conflict as a manifestation of failed management of disagreements, the higher are the chances of developing efficient conflict prevention measures.[35] Norm-making processes offer valuable opportunities for stakeholders to recognize the effects of limited trust between major powers and the means to overcome them. Regional organizations such as the OSCE were created as a response to the need observed by States to build trust and strengthen cooperation and are often regarded as holding the key to the impasse at the global level.[36]

Regional organizations have a long history of working with CBMs in conventional security areas.[37] The OSCE, the world's largest security-oriented regional organization, has a direct mandate to work on reducing risks of conflict in Europe, and successfully played the role it assumed in 2011 to strengthen cybersecurity.[38] In 2017, the OSCE had already developed sixteen practical and actionable measures in this area, which can be grouped into two main clusters: transparency and cooperation measures. These tools aim at enhancing cooperation, transparency, predictability, and stability, to reduce the risks of misperception, escalation, and conflict, that may stem from the use of ICTs.[39] These goals are tackled through information-sharing, improvement of national protective capacities, cooperation on incident response, and refrainment from destabilizing State practices.[40]

Due to its long history of promoting constructive dialogue, the OSCE is best suited to continuously respond to regional concerns or needs, not only of like-minded participating States, but also to bring together non-likeminded States which are in

[34] "ILC Draft Articles" note 20 above.
[35] Patryk Pawlak et. al., "Cyber Conflict Uncoded: The EU and Conflict Prevention in Cyberspace," *EUISS Brief* 7 (2020).
[36] *Id.*
[37] Among them, the OSCE and the Shanghai Cooperation Organization are widely regarded as the two most active. Baseley-Walker, "Transparency and Confidence-Building," 36; Hitchens and Gallagher, "Building Confidence in the Cybersphere," 4.
[38] The mandate of OSCE includes arms control, CBMs, human rights, press freedom, and fair elections.
[39] "OSCE Permanent Council (PC) Decision 1039," April 26, 2012, https://www.osce.org/pc/90169; "OSCE PC Decision 1106," December 3, 2013, http://www.osce.org/pc/109168; "OSCE PC Decision 1202," March 10, 2016, http://www.osce.org/pc/227281. [accessed 15.06.2021].
[40] Hitchens and Gallagher, "Building Confidence in the Cybersphere," 2.

different stages of cyber development.[41] OSCE's active efforts in shaping developments in the cyber domain, including setting the global tone for the development and operationalization of norms and CBMs, is broadly recognized by its partner organizations and in GGE reports.[42]

As the current OSCE's focus is to implement already agreed CBMs, rather than pursuing additional cyber norms, this paper aims at arguing several tools of effective consolidation.[43] First, this process should build on previously agreed principles and norms, and focus on issues which received broad support by individual States, or by parallel processes, such as the GGE. Although due diligence is not widely endorsed as a binding rule of international law, there is currently widespread support of this non-binding norm of responsible State behavior.[44] Voluntary non-binding norms can progressively acquire customary international law status, as well as third party endorsement. Efficient norms may generate productive imitation, especially if these are agreed by soft powers, as the espionage case illustrates.[45] Therefore, simplicity might be the key, by reaching political commitments among a group of like-minded actors, by operationalization of agreements and development of culturally grounded behavioral expectations.[46] The potential for practical implementation of CBMs makes them unique instruments, not just in the OSCE area, but as a source of good practices for other organizations to replicate.[47]

---

[41] For e.g., the agreement on detailed interpretation of major principles of international law during the 1975 Final Act of the Helsinki Conference on Security and Cooperation in Europe, the CBMs contained in the 1986 Stockholm Accord, and numerous election assistance and monitoring efforts. Baseley-Walker, "Transparency and Confidence-Building," 36; Velimir Radicevic, "Promoting Cyber Stability between States: OSCE Efforts to Reduce the Risks of Conflict Stemming from the Use of Information and Communication Technologies (ICTs) in the Context of Global and Regional Security," *OSCE Yearbook,* ed. IFSH (2018): 201.

[42] Pawlak et al., "Cyber Conflict Uncoded", note 34 above; Heli Tiirmaa-Klaar, "Two Generations of EU Cybersecurity Strategies," in *Handbook on Cybersecurity: The Common Security and Defence Policy of the European Union*, ed. Jochen Rehrl (Directorate for Security Policy of the Federal Ministry of Defence of the Republic of Austria, 2019), 18–26. "U.N. Document A/68/98*, Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security," June 24, 2013, http://www.un.org/ga/search/view doc.asp?symbol=A/68/9, [hereinafter GGE 2013 report]; "GGE 2015 report", note 18 above. [accessed 15.06.2021].

[43] Hitchens and Gallagher, "Building Confidence in the Cybersphere," 9.

[44] There are still concerns that its clarification offers opportunities for States to allege more breaches of international law and increase the frequency of countermeasures, which ultimately hamper stabilization of this international law principle in cyberspace. Eric T. Jensen and Sean Watts, "A Cyber Duty of Due Diligence: Gentle Civilizer or Crude Destabilizer?," *Texas Law Review* 95 (2017): 1573.

[45] Once the United States and China adopted a norm against commercial cyberespionage, both Germany and the United Kingdom undertook their own bilateral negotiations with China, and later the entire G-20 followed suit.

[46] Finnemore and Hollis, "Constructing Norms for Global Cybersecurity," 472.

[47] Radicevic, "Promoting Cyber Stability between States," 207.; "OSCE PC Decision 1106," note 39 above.

Second, the OSCE efforts escape many of the hurdles of high-level political commitments, including vague language, and focus on directive steps.[48] The stakeholders should identify and capitalize on the benefits of regional bodies, including their capacity to be more responsive to the changing environment, and the closed sessions with less public scrutiny, where States' concerns can be more effectively addressed.[49] Moreover, benefiting from an established Secretariat and attached procedures, States can adapt OSCE information-sharing platforms to even more robust frameworks. As a neutral organization, with a clear mandate, the OSCE can act as an objective forum, because it does not have defense or sanctioning prerogatives.

Third, the OSCE should capitalize on the participation of its stakeholders, which are States, primary actors of international law. While other norm-making laboratories, such as the Tallinn Manual 2.0, are influential resources, these multilateral efforts are criticized for only addressing the members of a particular system or alliance, and therefore, their lack of impact on States that are not involved in that process.[50] The USA and the Russian Federation, two of the States that are far apart on fundamental questions of application of international law to cyberspace, have participated in the GGEs and are standing members of the OSCE.

Fourth, strengthening the regional structures for conflict prevention requires a great amount of political will. However, for broader inclusion, coherence, and complementarity of efforts, and to avoid risks of duplication, international partners should enhance their cooperation at all working levels. More synergy among regional organizations will enhance common understanding of threats, exchange of lessons learned, and promote cooperation over competition. These efforts can provide advanced legal policy training for diplomats and local capacity building, which is crucial to follow-up on the implementation of CBMs. The OSCE should avail itself of the dialogue channels in place and establish new partnerships for a comprehensive picture of regional views and conflict prevention mechanisms.

Cyberpolicy cooperation and understanding of States' views and concerns should build on the significant overlap in membership of the EU, the OSCE, and NATO, organizations with highly complementary mandates. While the EU focuses on strengthening resilience through finance and diplomacy, the OSCE's model of regional security, and NATO's crisis management capacities could merge into meaningful synergies with the purpose of conflict prevention and early warning, common features of these organizations' mandates.[51]

---

[48] For e.g., in contrast to the GGE wording, such as "States should consider" and "States could", the OSCE used terms such as "will" and "shall", committing States to certain legal issues. "GGE 2013 report", note 42 above (Section IV, para 26c).

[49] Hitchens and Gallagher, "Building Confidence in the Cybersphere," 7.

[50] *Id.,* 5.

[51] Niklas Bremberg, "European Regional Organizations and Climate-related Security Risks: EU, OSCE and NATO," *SIPRI Insights on Peace and Security* no. 1 (2018): 13, https://www.sipri.org/publications/2018/sipri-insights-peace-and-security/european-regional-organizations-and-climate-related-security-risks-eu-osce-and-nato. [accessed 15.06.2021].

Although the OSCE process cannot force States to implement their recommendations, it can employ preventive and quiet diplomacy, as well as results-orientated dialogue to find common grounds on emerging security challenges.[52] As GGE processes share almost overlapping mandates with the OEWG, the OSCE can be among the most promising venues for multilateral cybersecurity cooperation. In this regard, the OSCE's ability to bring the United States and Russia to the conversation table is crucial, and with EU support, it should strive at engaging Chinese representatives as well. The People's Republic of China, which takes a similar view to Russia, also participated in the GGEs, but is not an OSCE member. The preliminary conversations should focus on national interpretations and application of fundamental international law principles. To ensure a candid exchange of views, initial conversations should be held under *Chatham House Rule* and avoid public scrutiny.

Fifth, as the coordinating fora for CBMs, the OSCE, has accumulated political capital of addressing States' reluctance regarding information-sharing and inherent challenges that create multi-stakeholder cooperation problems. During the previous rounds, the OSCE gained an overview on which objectives can reasonably be achieved multilaterally, and which ones are more suited for bilateral cooperation mechanisms.[53] Deriving lessons learned from past processes enables better approaches to national interests, concerns, and operational practices.[54]

It would be utopic to believe that major powers will agree on interpretations of every legal institution. Even the experts of the Tallinn Manual Process could not agree on basic principles, although as mentioned, they mainly originated from like-minded states and cultures. The first part of this paper highlighted that the process of norm-creation may matter as much as the destination, as participants agree to disagree and understand each other's differences and underlying rationales.

Another important endeavor is the analysis of past and present challenges of effective implementation of voluntary norms. The OSCE should strive at assisting States to recognize the prospective domestic and foreign policy value of recognizing CBMs.[55] The reasons why some of the measures were perceived as being less important, implementation challenges, and responses within the civil society and industry shall be thoroughly examined.

The Proliferation Security Initiative (PSI) is sometimes cited as a possible model for future cybersecurity cooperation. [56] This approach has been described as

---

[52] "Perspectives of the UN & Regional Organizations on Preventive and Quiet Diplomacy, Dialogue Facilitation and Mediation. Common Challenges & Good Practices," *Workshop Report OSCE* (February 2011), https://peacemaker.un.org/sites/peacemaker.un.org/files/PerspectivesonPreventiveandQuietDiplomacy_OSCE2011_0.pdf [accessed 15.06.2021].

[53] Hitchens and Gallagher, "Building Confidence in the Cybersphere," 2.

[54] Radicevic, "Promoting Cyber Stability between States," 211.

[55] *Id.,* 209*;* The nominal implementation rate across all CBMs by participating States is high, each State having implemented at least one measure.

[56] In sum, in 2002, a North Korean freighter, transited the Arabian Sea without flying a flag and with a newly painted hull that obscured its name and home port. U.S. intelligence officials asked Spanish marines to board and search the ship as a "stateless" vessel. On board, they discovered missiles

a "coalition of the willing" against a global threat by means of flexible coordination of national and international instruments.[57] The proposed institutional architecture encourages collective action for a common cause, without requiring legally binding commitments. This agreement is also recognized for reaching a political commitment by only a few States, which accepted that they have different capacities and resources to identify and respond to threats. This initiative represents a successful example of voluntary cooperation, first among like-minded States, around enforcement of specific, agreed norms of behavior.

The OSCE participating States should capitalize on lessons learned to operationalize norms in a practical manner, such as was the case of the 1990 OSCE Vienna Document on Negotiations on CSBMs, which contained voluntary military measures aiming at enhancing transparency, trust building, and arms control. After their translation into the cyber realm, these tools departed from the traditional military components of CSBMs and adopted more cyber diplomacy approaches, bringing both likeminded and non-likeminded States to the table.[58]

4.2 OSCE work and pressing cyberthreats

Part III of the paper detailed why States' recognition of their due diligence obligations is crucial for early warning, a key element of OSCE mandate. While the previous section suggested some practical steps for addressing this principle and other delicate cyber issues on which previous efforts have not concluded with unanimous consent, this section will emphasize why the most pressing issues require immediate attention.

First, the solid inter-state cooperation structure provided by OSCE should be utilized to build on pre-existing commitments to strengthen existing CBMs related to due diligence and launch legal and political conversations on the *preventive aspect* of this principle.[59] This process should include civil society and industry

hidden under bags of cement and unsuccessfully tried to seize them. Among law of the sea issues, this episode raised questions on States' collective capability to address the proliferation of weapons of mass destruction (WMD), their delivery systems, and related goods. In the aftermath of this event, the U.S. and Spain along with nine other States founded the Proliferation Security Initiative (PSI), a joint effort to strengthen the political commitment, practical capacities, and legal authorities necessary to stop, search, and, if necessary, seize vessels and aircraft believed to be transporting WMD. Unlike a traditional treaty, the PSI was agreed by virtue of States endorsing a political commitment, the *Statement of Interdiction Principle*s (SIP), which directs that all PSI activities should occur only to the extent consistent with an endorsing State's national laws and its obligations under international law. To date, more than 100 States have endorsed the SIP. This description was adapted after Duncan B. Hollis and Matthew C. Waxman, "Promoting International Cybersecurity Cooperation: Lessons from the Proliferation Security Initiative (PSI)," *Temple University Beasley School of Law, Legal Studies Research Paper* no. 3 (2018):3.

[57] *Id.,* 6.

[58] Radicevic, "Promoting Cyber Stability between States," 204.

[59] "OSCE PC Decision 1106," note 38 above. CBM 5 affirms States commitment to "use the OSCE as a platform for dialogue, exchange of best practices […] including effective responses to related threats." Moreover, further dialogue on interpretation of due diligence obligations is in line with CBM 9, which addresses the lack of agreed terminology. Consolidating the due diligence principle

representatives, who can provide fresh insight on the realistic capabilities of states to commit, on the requirements and obstacles to full implementation.

Second, development of agreed terminology is fundamental for pursuing further dialogue, as States can identify areas of agreement and disagreement about the translation of the due diligence principle from other areas of law, such as space law, environmental law, or law of the sea.[60] The same rationale applies to divergent views in regard to terminology of "essential" or "critical" infrastructure and associated concerns. In most views, a cyber intrusion against ordinary hospitals, patients' databases or laboratories would not impact national care during ordinary times.[61] However, given the shortages of medical infrastructure during the 2020 pandemic, the threshold for the "essential character" would likely shift. While an infectious disease hospital or testing facility are expected to be considered indispensable medical services during a pandemic, the legal effects of deaths occurring as indirect consequences of cyber intrusions remain unanswered.[62] Perhaps, the silver lining of recent malicious cyberoperations is the opportunity for States and multilateral fora to clarify application of international law, endorse norms, and assert their credibility.[63]

5. Conclusion

The digital arms race determined numerous States to enhance their defensive and offensive cyber capabilities, and some already defined cyberspace as a military domain. The future will tell whether an equivalent of the "Treaty on Open Skies" is possible in cyberspace.[64] With the same goal, the value of CBMs is rendered by their mere purpose, to create safe and predictable behavior in cyberspace, and to build a culture of transparency among stakeholders. This paper highlighted the value of interregional cooperation on cybersecurity and the need to institutionalize these

in cyberspace reflects CBM 4, which established voluntary information-sharing on measures States have taken to ensure an open, interoperable, secure, and reliable Internet.

[60] "OSCE PC Decision 1202," note 39 above. Building on CBM 15, the OSCE can provide a solid platform where States can discuss and identify examples of critical infrastructure.

[61] In an analysis of the contextual determination of necessity and essentiality according to the law of state responsibility, the director of the Tallinn Manual Project examined the seriousness of cyber operations against medical infrastructure. In his view, the gravity of these operations depends on alternative systems that ensure continuation of medical treatment, and on determination of medical infrastructure as "essential" in the specific context. Michael N. Schmitt, "Peacetime Cyber Responses and Wartime Cyber Operations Under International Law: An Analytical Vade Mecum," *Harvard National Security Journal* 8, no. 2 (2017): 252.

[62] For example, the U.K. endorses the possibility of applying the principle on non-intervention to cyber actions against "essential medical services." Jeremy Wright, "Cyber and International Law in the 21st Century," at *Chatham House Royal Institute*, May 23, 2018, https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century. [accessed 15.06.2021].

[63] Adina Ponta, "Hostile Cyberoperations Against Medical Facilities and Their Impunity," *Jurist Legal News and Research,* May 22, 2020, https://www.jurist.org/commentary/2020/05/adina-ponta-hospital-hostile-cyberoperations/. [accessed 15.06.2021].

[64] Radicevic, "Promoting Cyber Stability between States," 202; "Treaty on Open Skies," https://www.osce.org/files/f/documents/1/5/ 14127.pdf. [accessed 15.06.2021].

dialogues, to operationalize implementation measures, and strengthen commitments. Despite their slow pace, CBMs are continuously developed with every State action or declaration, having a great potential to uphold international peace and reduce risks of conflict and escalation. Norms of responsible State behavior seek to define key concepts, such as "red lines" for the use of ICTs.[65] One of the most important thresholds is that States make sure that the territory or cyber infrastructure under their control is not used for operations that affect the rights of, and produce adverse consequences for, other States.

The 2017 GGE demonstrated that there are no guarantees of reaching international consensus for the creation of norms to secure and govern cyberspace. Security threats are inherently transnational, and their prevention and mitigation will require greater engagement and commitment from the international community. Their successful approach will imply constructive and open conversations among various stakeholders with divergent priorities, agendas, and views on international law. At this moment in time, progress requires continuous compromise by the major powers, which sometimes express contrasting interpretations of international law applicable to cyberspace. OSCE's contribution and assistance to constructive dialogue, flexible understanding of legal views, and creation of national practices that allow implementation is crucial. This model of cooperation, the norm-setting and CBMs are a model for other regional organizations and their image should be defended by continuous efforts.

Bibliography

I. Books

1. Radicevic, Velimir. "Promoting Cyber Stability between States: OSCE Efforts to Reduce the Risks of Conflict Stemming from the Use of Information and Communication Technologies (ICTs) in the Context of Global and Regional Security." In *OSCE Yearbook,* edited by IFSH (2018): 201-212.
2. Schmitt, Michael N. ed. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge: Cambridge University Press, 2017. doi:10.1017/9781316822524.
3. Stockburger, Peter Z. "From Grey Zone to Customary International Law: How Adopting the Precautionary Principle May Help Crystallize the Due Diligence Principle in Cyberspace" in *NATO CCD CoE Publications*, eds. T. Minárik, R. Jakschis, and L. Lindström (2018): 245-262.
4. Tiirmaa-Klaar, Heli. "Two generations of EU cybersecurity strategies." In *Handbook on Cybersecurity: The Common Security and Defence Policy of the European Union*, edited by Jochen Rehrl, 18-26. Directorate for Security Policy of the Federal Ministry of Defense of the Republic of Austria, 2019.

[65] *Id.,* 203.

II. Articles

1. Bannelier, Karine. "Cyber Diligence: A Low-Intensity Due Diligence Principle for Low-Intensity Cyber Operations?" *Baltic Yearbook of International Law* 14 (2014): 1-15.
2. Bannelier, Karine, and Theodore Christakis. "Cyber-Attacks: Prevention-Reactions: The Role of States and Private Actors." *Les Cahiers de la Revue Défense Nationale* (2017): 7-86.
3. Baseley-Walker, Ben. "Transparency and Confidence-Building Measures in Cyberspace: Towards Norms of Behaviour." *Confronting cyberconflict* no. 4 (2011): 31-40. https://citizenlab.ca/cybernorms 2012/Baseley Walker2011.pdf.
4. Berkes, Antal. "Human Rights Obligations of the Territorial State in the Cyberspace of Areas Outside Its Effective Control." *Israel Law Review* 52, no. 2 (2019): 197-231.
5. Besson, Samantha. "Due Diligence and Extraterritorial Human Rights Obligations – Mind the Gap!" *ESIL Reflections* 9, no. 1 (2020): 1–9. https://esil-sedi.eu/wp-content/uploads/2020/04/ESIL-Reflection-Besson-S.-3.pdf.
6. Bremberg, Niklas. "European Regional Organizations and Climate-related Security Risks: EU, OSCE and NATO." *SIPRI Insights on Peace and Security* no. 1 (2018). https://www.sipri.org/publications/2018/sipri-insights-peace-and-security/european-regional-organizations-and-climate-related-security-risks-eu-osce-and-nato.
7. Corn, Gary P., and Robert Taylor. "Sovereignty in the Age of Cyber." *American Journal of International Law Unbound* 111 (2017): 207–212. doi:10.1017/aju.2017.57.
8. Eichensehr, Kristen. "The Cyber-Law of Nations." *Georgetown Law Journal* 103, no. 2 (2015): 317-380.
9. Finnemore, Martha, and Duncan B. Hollis. "Constructing Norms for Global Cybersecurity." *American Journal of International Law* 110, no. 3 (2016): 425-479.
10. Heupel, Monika. "How do States Perceive Extraterritorial Human Rights Obligations? Insights from the Universal Periodic Review." *Human Rights Quarterly* 40, no. 3 (2018): 521-546.
11. Hitchens, Theresa, and Nancy W. Gallagher. "Building Confidence in the Cybersphere: A Path to Multilateral Progress." *Journal of Cyber Policy* 4, no. 1 (2011): 4-21. http://doi.org/10.1080/23738871.2019.1599032.
12. Hollis, Duncan B, and Matthew C. Waxman. "Promoting International Cybersecurity Cooperation: Lessons from the Proliferation Security Initiative (PSI)." *Temple University Beasley School of Law, Legal Studies Research Paper* no. 3 (2018): 1-14.
13. Jensen, Eric Talbot. "The Tallinn Manual 2.0: Highlights and Insights." *Georgetown Journal of International Law* 48 (2017): 735-778.
14. Jensen, Eric T., and Sean Watts. "A Cyber Duty of Due Diligence: Gentle Civilizer or Crude Destabilizer?" *Texas Law Review* 95 (2017): 1555-1577.
15. Kilovaty, Ido. "An Extraterritorial Human Right to Cybersecurity." Notre Dame Journal of International and Comparative Law" 10, no.1 (2020): 35-55.
16. Roguski, Przemyslaw. "Application of International Law to Cyber Operations: A Comparative Analysis of States' Views." *Policy brief* (2020): 1-48.
17. Schmitt, Michael N. "Grey Zones in the International Law of Cyberspace." *The Yale Journal of International Law Online* 42, no. 2 (2017).
18. Schmitt, Michael N. "Peacetime Cyber Responses and Wartime Cyber Operations Under International Law: An Analytical Vade Mecum." *Harvard National Security Journal* 8, no. 2 (2017): 239-282.
19. Schmitt, Michael N., and Liis Vihul. "Respect for Sovereignty in Cyberspace." *Texas Law Review* 95, no. 7 (2017): 1639-1671.

20. Shackelford, Scott J., Scott Russell, and Andreas Kuehn. "Unpacking the International Law on Cybersecurity Due Diligence: Lessons from the Public and Private Sectors." *Chicago Journal of International Law* 17, no.1 (2016):1-50.

III. Web sources

1. Moynihan, Harriet. "The Application of International Law to State Cyberattacks: Sovereignty and Non-Intervention." *Chatham House Research Paper* (2019). https://www.chathamhouse.org/sites/default/files/ publications/research/2019-11-29-Intl-Law-Cyberattacks.pdf.
2. Pawlak, Patryk, Eneken Tikk, and Mika Kerttunen. "Cyber Conflict Uncoded: The EU and conflict prevention in cyberspace." *EUISS Brief* 7 (2020).
3. Pawlak, Patryk and Thomas Biersteker eds. "Laws of gravitation. Due diligence obligations in cyberspace." In *EU Cyber Sanctions and Norms in Cyberspace*. Chaillot Paper 155 (2019). https://www.iss.europa.eu/sites/ default/files/EUISSFiles/cp155.pdf.
4. Ponta, Adina. "Cyber Operations Against Medical Facilities During Peacetime." *Lawfare Blog,* May 1, 2020. https://www.lawfareblog.com/cyber-operations-against-medical-facilities-during-peacetime.
5. Ponta, Adina, "Hostile Cyberoperations Against Medical Facilities and Their Impunity." *Jurist Legal News and Research,* May 22, 2020. https://www.jurist.org/commentary/ 2020/05/adina-ponta-hospital-hostile-cyber operations/.
6. Ponta, Adina. "Security and Human Rights Challenges of Cyber Due Diligence." *Harvard International Law Journal Online* (2020). https://harvardilj.org/2020/06/ security-and-human-rights-challenges-of-cyber-due-diligence/.
7. Ruhl, Christian, Duncan Hollis, Wyatt Hoffman, and Tim Maurer. "Cyberspace and Geopolitics: Assessing Global Cybersecurity Norm Processes at a Crossroads." *Carnegie Endowment for International Peace Working Paper* (2020): 1-25. https://carnegieendowment.org/files/Cyberspace_and_Geopolitics.pdf.
8. Schmitt, Michael. "The Netherlands Releases a Tour de Force on International Law in Cyberspace: Analysis." *Just Security*, October 14, 2019. https://www.justsecurity.org/ 66562/the-netherlands-releases-a-tour-de-force-on-international-law-in-cyberspace-analysis/.
9. Przemyslaw Roguski. "Application of International Law to Cyber Operations: A Comparative Analysis of States' Views." *The Hague Program for Cyber Norms Policy brief,* March 2020, https://www.thehaguecybernorms. nl/research-and-publication-posts/application-of-international-law-to-cyber-operations-a-comparative-analysis-of-states-views.
10. Wright, Jeremy. "Cyber and International Law in the 21st Century." Chatham House Royal Institute (2018). https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century.

IV. Legal and public documents

1. "Annex to General Assembly Resolution 56/83 of December 12, 2001, corrected by document A/56/49 (Vol. I) /Corr.4." Responsibility of States for Internationally Wrongful Acts, 2001, https://legal.un.org/ilc/texts/ instruments/english/draft_articles/ 9_6_2001.pdf
2. "Cybersecurity Strategy. Republic of Estonia 2019-2022." *Ministry of Economic Affairs and Communications.* February 2018. https://www.mkm.ee/sites/default/files/ kyberturvalisuse_strateegia _2022_eng.pdf.

3. "Declaration by the High Representative Josep Borrell, on behalf of the EU, on malicious cyber activities exploiting the coronavirus pandemic." *Press Release* 26/120, April 30, 2020. https://www.consilium.europa.eu/en/press/press-releases/2020/04/30/declaration-by-the-high-representative-josep-borrell-on-behalf-of-the-european-union-on-malicious-cyber-activities-exploiting-the-coronavirus-pandemic/.
4. "Dutch National Cyber Security Agenda." *The Netherlands' Ministry of Justice and Security*. April 2018. https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/national-cyber-security-strategy-1.
5. European Court of Human Rights. *López Ostra v. Spain,* Application no. 16798/90 (2004).
6. European Court of Human Rights. *Osman v. The United Kingdom,* Case no. 87/1997/871/1083 (1998).
7. "Global Conference on Cyber Space (GCCS) 2017." *Internet Society*, November 23-24, 2017. https://www. internetsociety.org/events/gccs-2017/.
8. "G-8 Declaration Renewed Commitment for Freedom and Democracy." *G-8 Summit of Deauville*, May 2011. https://www.nato.int/nato_static/assets/pdf/pdf_2011_05/20110926_110526-G8-Summit-Deauville.pdf.
9. "G-20 Leaders' Communique´." *Antalya Summit*, November 15-16, 2015. http://www.mofa.go.jp/files/00011 1117.pdf.
10. International Court of Justice. *Case Concerning Pulp Mills on the River Uruguay (Argentina v. Uruguay),* April 20, 2010.
11. International Court of Justice. Judgement *Certain Activities Carried Out by Nicaragua In the Border Area (Costa Rica V. Nicaragua),* December 16, 2015.
12. "International Covenant on Economic, Social and Cultural Rights." *Adopted and opened for signature, ratification and accession* December 16, 1966, U.N.G.A Resolution 2200A (XXI) (entered into force Jan. 3, 1976). https://www.ohchr.org/en/professionalinterest/pages/cescr.aspx.
13. International Tribunal for the Law of the Sea. Request for Advisory Opinion submitted to the Seabed Disputes Chamber, *Responsibilities and Obligations of States Sponsoring Persons and Entities with Respect to Activities in the Area*, February 1, 2011.
14. "London Process", formally called "Global Conference on Cyber Space." Global Forum on Cyber Expertise accessed June 28, 2020. https://www.thegfce.com/about/gccs.
15. "Maastricht Principles on the Extra-Territorial Obligations of States in the area of Economic, Social and Cultural Rights." (2011). https://www.ciel.org/wp-content/uploads/2015/05/Maastricht_ETO_ Principles_21Oct11.pdf.
16. "National Cyber Strategy of the United States of America." *The White House*. September 2018. https://www. whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf.
17. "OSCE Permanent Council Decision 1039." April 26, 2012. https://www.osce.org/pc/90169.
18. "OSCE Permanent Council Decision 1106." December 2013. http://www.osce.org/pc/109168.
19. "OSCE Permanent Council Decision 1202." March 10, 2016. http://www.osce.org/pc/227281.
20. "Perspectives of the UN & Regional Organizations on Preventive and Quiet Diplomacy, Dialogue Facilitation and Mediation. Common Challenges & Good Practices." *Workshop Report OSCE* (2011). https://peacemaker. un.org/sites/peacemaker.un.org/files/PerspectivesonPreventiveandQuietDiplomacy_OSCE2011_0.pdf.

21. Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, *Official Journal of the European Union*, L 119/1 (April 27, 2016).
22. Speech, President Kersti Kaljulaid. "President of the Republic at the opening of CyCon 2019." May 29, 2019. https://www.president.ee/en/official-duties/speeches/15241-president-of-the-republic-at-the -opening-of-cycon-2019/index.html.
23. "Stay Smart. Stay Safely Connected." *Cybersecurity Tech Accord.* (May 2020). https://cybertech accord.org/.
24. "Strategic Review of Cyber Defence." *Repulique Francaise - Secrétariat Général de la Défense et de la Sécurité Nationale.* February 2018. http://www.sgdsn.gouv.fr/uploads/2018/03/revue-cyber-resume-in-english.pdf.
25. "The UK National Cyber Security Strategy 2016-2021." *HM Government*, 2016. https://assets.publishing. service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf.
26. "The 9 Principles." Paris Call, December 11, 2018. https://pariscall.international/en/supporters.
27. "U.N. Document A/56/10." International Law Commission: Prevention of Transboundary Harm from Hazardous Activities with commentaries, Article 3, commentary (9) (2001). https://legal.un.org/ilc/texts/instruments/english/commentaries/9_7_2001.pdf.
28. "U.N. Document A/68/98*." Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. June 24, 2013. http://www.un.org/ga/search/view_ doc.asp?symbol=A/68/9.
29. "U.N. Document A/69/723, International Code of Conduct for Information Security." in *Letter from the Permanent Representatives of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan to the United Nations Secretary-General,* January 9, 2015. https://digitallibrary.un.org/record/78684 6/files/A_69_723-EN.pdf.
30. "U.N. Document A/70/174. Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security.", July 22, 2015. https://undocs.org/A/70/174.
31. "U.N. Document CCPR/C/21/Rev.1/Add. 1326." International Covenant on Civil and Political Rights. General Comment No. 31." Human Rights Committee (HRC), May 2004. http://docstore.ohchr.org/Self Services/Files Handler.ashx?enc=6QkG1d%2FPPRiCAqhKb7yhsjYoiCfMKoIRv2FVaVzRkMjTnjRO%2Bfud3cPVrcM9YR0iW6TxaxgP3f9kUFpWoq%2FhW%2FTpKi2tPhZsbEJw%2FGeZRASjdFuuJQRnbJEaUhby31WiQPl2mLFDe6ZSwMMvmQGVHA%3D%3D.
32. "U.N. Document E/C.12/2000/4." CESCR General Comment No. 14: The Right to the Highest Attainable Standard of Health (Art. 12) August, 11, 2000.
33. "U.N. General Assembly, Resolution 73/266, Advancing Responsible State Behaviour in Cyberspace in the Context of International Security." A/RES/73/266 (December 22, 2018). https://undocs.org/pdf?Symbol=en/A/ RES/73/266.
34. "U.N. Reports of International Arbitral Awards, 2006 Permanent Court of Arbitration." *Trail smelter case* (*United States v. Canada*). https://legal.un.org/riaa/cases/vol_III/1905-1982.pdf.
35. "2013 Istanbul Final Declaration and Resolution on Cyber Security." *OSCE Parliamentary Assembly*, June 29-July 3, 2013, https://www.oscepa.org/meetings/annual-sessions/2013-istanbul-annual-session/2013-istanbul-final-declaration/1652-15.